Digital Whisper
Technologic Papers

הדרך הארוכה להסמכת CISSP

מאת דודו ברודה

הקדמה

מהי הסמכת ה-CISSP ולמה צריך אותה?

פירושם של ראשי התיבות: Certified Information Systems Security Professional. מדובר בהסמכה בתחום אבטחת המידע הידועה ביותר בעולם (וגם בארץ). (לקריאה ב-Wikipedia).

מכיוון שמדובר בהסמכה נייטרלית (לא קשורה לאף יצרן) ושהיא קשה (מאוד) להשגה, אין ספק שלהחזיק אותה מהווה סוג של תעודת ביטוח עבור העולם (לבעל ההסמכה יש ניסיון וידע בתחום). כל מי שרוצה להתקדם בתחום אבטחת המידע חייב לפחות לשקול לגשת למבחן בשלב כזה או אחר (הרבה מומחים בתחום מחזיקים בהסמכה). אישית קיבלתי את החלטה בגלל האתגר, רציתי לדעת האם אני יכול לעבור את המבחן דרך לימוד עצמאי (ללא קורס), רק על בסיס ידע, ניסיון והכנה רצינית.

מטרת המאמר הבא היא לא להסביר מהי ההסמכה, לכן אני מעדיף להפנות אתכם למאמרים שמסבירים בצורה טובה מהי ההסמכה ומשמעותה: כאן מ-NewsGeek וממכללת See-Security.

מה מטרת המאמר ?

כשהחלטתי לעבור את הסמכת ה-CISSP חיפשתי ברשת מידע בעברית על המבחן. לצערי הרב, בזמנו לא מצאתי אף מאמר רלוונטי בשפה העברית. לאחר קבלת ההסמכה, החלטתי "לתקן" את המצב ולפרסם מדריך בעברית.

מטרת המאמר היא לספק סקירה כללית על תהליך קבלת ההסמכה ודרכי הכנה למבחן, בעיקר במידה ומחליטים להתכונן לבד (ללא קורס הכנה).

מהן דרישות ההסמכה?

צריך להבחין בין ההסמכה לבין המבחן. הצלחה במבחן היא רק חלק מדרישות קבלת ההסמכה. כדי לקבל את ההסמכה, יש לעמוד בכל תנאי הסף שהוגדרו על ידי ארגון ISC2.

ניסיון: נדרשות חמש שנות עבודה מלאות בשניים מעשרת תחומי המבחן. ניתן לגשת למבחן בלי לעמוד בתנאי זה אבל במקרה של הצלחה, המועמד יאלץ להמתין עד לצבירת הניסיון הנדרש (סטטוס של "ISC2 Associate"). מחזיקי הסמכות מוכרות בתחום יכולים לקבל הקלה של שנה בדרישת הניסיון אם ההסמכה שלהם מוכרת ע"י ISC2 (קישור לרשימה של ההסמכות המוכרות).

מבחן: קשה ויקר (ראו תמחור מדויק בסוף הכתבה). המבחן ללא ספק הקשה ביותר שעברתי בחיים. שש שעות, 250 שאלות אמריקאיות... כמעט כולן מבלבלות. הדרישה היא לענות לכל שאלה עם התשובה הנכונה ביותר (יתכנו כמה תשובות נכונות... יש רק אחת שהיא הנכונה ביותר). חייבים לקבל 700 נקודות מתוך 1000 כדי לעבור (יש משקל משתנה לשאלות, לא ברור מהם פקטורים הנוסחה של הציון, מדובר בסוד של ארגון ISC2).

Endorsement: לאחר הצלחה במבחן, נדרש המועמד למלא טופס ולהחתים Endorser - מישהו בעל ההסמכה בתוקף ("in good standing"). ה-Endorser מהווה אישור על נכונות דיווחי המועמד, בעיקר לגבי ההצרות הקשורות לניסיון המקצועי (ה-Endorser שלי יצר קשר עם הבוס כדי לאמת את הנתונים). עדיף לבחור במישהו שמכיר את המועמד. למועמד שלא מכיר אף מוסמך ניתן האפשרות לבצע את התהליך ישירות מול ארגון ISC2 (הסבר כאן). התהליך יכול לקחת עד שישה שבועות.

חתימה על הקוד האתי של ISC2: נדרשת הסכמה של המועמד לעמוד בקוד האתי של הארגון (פירוט באתר של ISC2). טיפ קטן: כדאי להכיר אותו טוב מכיוון שחלק קטן מהשאלות במבחן מתייחסות ישירות לקוד האתי.

Audit (בחירה אקראית של חלק מהמועדמים): לא מתקיים תמיד אבל יתכן והמועמד ייבחר לבדיקה נוספת של נתוני הרקע שלו, כגון ניסיון והצהרות אחרות (בדומה ל-Endorsement).

איך מתכוננים למבחן?

יש שתי דרכים להתכונן למבחן:

- להרשם לקורס או לסדנת הכנה:

בארץ ישנן מספר מכללות שמתמחות בהכנה למבחן ה-CISSP. אישית אני ממליץ על מכללת SEE-SECURITY, הנציגה הרשמית של ISC2 בישראל (**גילי-נאות**: אני בעצמי מרצה במכללה). חשוב לציין שניתן ללמוד בקורסים ברשת (יקר מאוד יחסית ורק באנגלית כמובן): אזכיר את הקורסים של SANS ושל ISC2.

- ללמוד לבד:

כן, כן... יש משוגעים כמוני שעושים את ההכנה לבד, על בסיס ספרים, גלישה ברשת (Google הוא חבר) ופגישות לימוד (אם אתם מכירים עוד משוגעים). זאת הדרך הקשה אבל אם עוברים, התענוג והשמחה גדולים בהרבה מאשר מי שלמד בקורס ☺, נדרשת משמעת עצמית ברמה גבוהה מכיוון שההכנה פרוסה על גבי חודשים (במקרה הטוב).

איפה מוצאים חומר לימוד?

כדאי להתחיל את המסע באיסוף חומר הלימוד. במידה והמועמד לומד דרך מכללה, יש סיכוי טוב שהוא יקבל ספרים וחומרים במסגרת הקורס.

ספר הלימוד: זהו הבסיס. לא ניתן לתכנן את המבחן בלי ספר אחד לפחות שמרכז את עשרת תחומי הלימוד, טיפים והסברים.

בזמנו, גלשתי ברשת ומצאתי שלושה ספרים שמוכרים כמצטיינים בנושא.

- **הספר הרשמי של ISC2 - "**ה-CBK**"** - מאוד מקיף אבל לא נוח לקריאה (כ-75/80$). הגרסה השלישית פורסמה בינואר 2012.

- **CISSP AIO** של הגורו האמריקאי Shon Harris - שון האריס מדהימה בכתיבה שלה. אפשר ללמוד בצורה כיפית. מאוד מומלץ.

- **CISSP For Dummies** - מעניין וקל לקריאה יחסית (כ-40$) אבל פחות נוח מ-AIO. הגרסה העדכנית הינה הרביעית (מאוגוסט 2012)

טיפ קטן: לא לרכוש את הספרים בחנות הרשמית שלהם, גשו ל-Ebay או Amazon ותחסכו עד עשרות דולרים.

אוסף של שאלות לתרגול:

אחת המשימות המרכזיות בהכנה היא ללמוד להתמודד עם אופי השאלות של ISC2.

אין דרך להתחמק מזה, תשכחו מכל רעיון "יצירתי" כמו למצוא Braindumps ברשת (זה לא מבחן של מייקרוסופט!) ברשת - **הם פשוט לא קיימים!**

- CCCure Quizzer (של Claude Dupuis) - אתר נהדר עם מאות ואולי אלפי שאלות. חלקן בחינם, חלקן בתשלום. חלק מהשאלות לא רלוונטיות אך זהו מקור טוב ללימוד.

- Security University Free Practice Tests - חינם (נדרש רישום - שימו לב שמייל האישור לא מזוהה כ-SPAM). מאגר שאלות יפה. שאלות מחולקות בקבוצות של: 10- 25 - 50 - 75 - 150 - 100 - 200. לפי תחומים (Domains) או כללי. מומלץ מאוד.

- Eric Conrad's 500 questions - שתי סימולציות מלאות בחינם, כולל הסברים. רמה טובה. אסור לפספס.

- CISSP MP3 and Quiz File (של Shon Harris) - הדבר הקרוב ביותר למבחן האמיתי. יקר (300$) אבל החומר איכותי (אפשר למצוא יד שניה ברשת - Ebay וכו').

- Studiscope self assessment (של ISC2) - מאוד יקר ($129 ל-100 שאלות או $289 ל-300 שאלות). שאלות אמתיות של מבחני העבר (יצאו מהמאגר). לא נוסה.

- CISSP Exam practice - לא יקר יחסית לאחרים ($59 למאות שאלות) אבל לפי דעתי השאלות קלות מדי ביחס למבחן ולשאר האתרים. למרות זאת, לאתר זה יש שם טוב בקהילת הלומדים.

- Techexams.net - חינם אבל רק כמה שאלות - כדאי לנצל.

- Knowledgebuster - כ-60 שאלות בחינם - כדאי לנצל.

- CISSP for Dummies app for iPhone - כ-$9.99 - מאוד נוח ללימוד נייד - שווה.

כמה זה עולה?

קודם כל, המבחן: עלות הרישום הינה גבוהה מאוד. כל רישום עולה $599 (פעם הייתה הנחה ברישום מוקדם, כבר לא קיימת מאז סוף 2012) - ראו פרסום מאתר ISC2. אם בטעות לא עברתם בפעם הראשונה, יש לשלם שוב.

קורסים במכללות יקרים אבל הם עושים את העבודה ומרכזים את החומר בצורה טובה מאוד (חיסכון בשעות חיפוש חומר, לא בשעות לימוד בבית). תתקשרו למכללות כדי לברר את המחיר ואת החומר שהן מספקות לסטודנט. חשוב לציין שקורס מסודר נותן גישה למרצה שתמיד יידע לספק טיפים והסברים מקצועיים, ערך מוסף חשוב.

ספרים עולים בין $30 ל-$70, אישית אני ממליץ שוב לרכוש את AIO של Shon Harris. יש בו כל מה שמועמד צריך לדעת ויותר.

יש מאגרי שאלות בחינם ויש מאגרים שעולים כסף. ממליץ להשקיע בגרסה בתשלום של CCCure Quizzer (במחיר של $39.99 עבור חצי שנה של שימוש). הרבה מאוד שאלות ומעקב צמוד לאורך הלימוד (הצגת אחוזי הצלחה לפי מבחן וסה"כ). ממליץ גם על CISSP for Dummies app for iPhone (במחיר של $19.99) כדי לנצל זמני נסיעות או המתנה מחוץ לבית בלימוד.

אישית, השקעתי בסביבות ה-$700 בסה"כ (כולל תשלום למבחן). זול יחסית.

איך לומדים מאחרים - טיפים להצלחה?

כשהחלטתי לגשת למבחן, התחלתי לחפש ברשת מאמרים, טיפים וסיפורי הצלחה כדי ללמוד איך להתכונן למבחן. אני משתף אתכם בקישורים שעזרו לי גם מבחינת החומר וגם פסיכולוגית:

- Clement's presentation (של Clement Dupuis) - קצת ישן (משנת 2007) אבל חובה לעבור על ההרצאה. הסבר יפה מאוד על החומר באופן כללי ועל תהליך ההסמכה.
- CBK Domain Previews (של ISC2) - הצגות של תחומי הלימוד ב-Webcasts. כדאי לראות, חינם
- Simplilearn presentation - של מכללה בעלת קורס הכנה. קצת משעמם (קול מעצבן) אבל חינם
- SANS Webcast - בנושא How to be Successful at Passing the CISSP (של Dr. Eric Cole) - הרצאה נהדרת שמסבירה את המורכבות ואת אופי המבחן (נדרשת יצירת משתמש באתר SANS, חינם).
- אתר Cccure.org (של Clement Dupuis) - חובה, אוסף של מאמרים, טיפים, שיתופי פעולה בין מועמדים.
- A journey into hell. My CISSP experience (של Marts McFly) - סיפור הצלחה של בחור נחמד. טיפים ואפילו קצת מצחיק (אשתו איימה עליו ברצח אם ייכשל).
- How I prepared my CISSP exam (של Didier Stevens) - מעבר לבלוג הנחמד, סיפור המבחן של Didier Stevens.
- I passed. Such a relief! (של Roman Zeltser) - מזדהה עם Roman במילה ומילה.
- My Top 10 Tips For Preparing and Passing the CISSP Exam (של Tony Bradley) - טיפים טובים.
- Preparing for the CISSP Exam (של Daniel A. Mroz) - סיפור וטיפים.
- CISSP Study Notes (של Andreas Athanasoulias) - קישור למסמכי עזר שכתב Andreas (סגנון CRAMS).

וכמובן, חייבים ללמוד מהניסיון של האחרים דרך הפורומים: גשו גם לפורומי CISSP של cccure.org (נדרש רישום חינם) וגשו גם לקבוצות עניין ב-Linkedin (כאן וכאן).

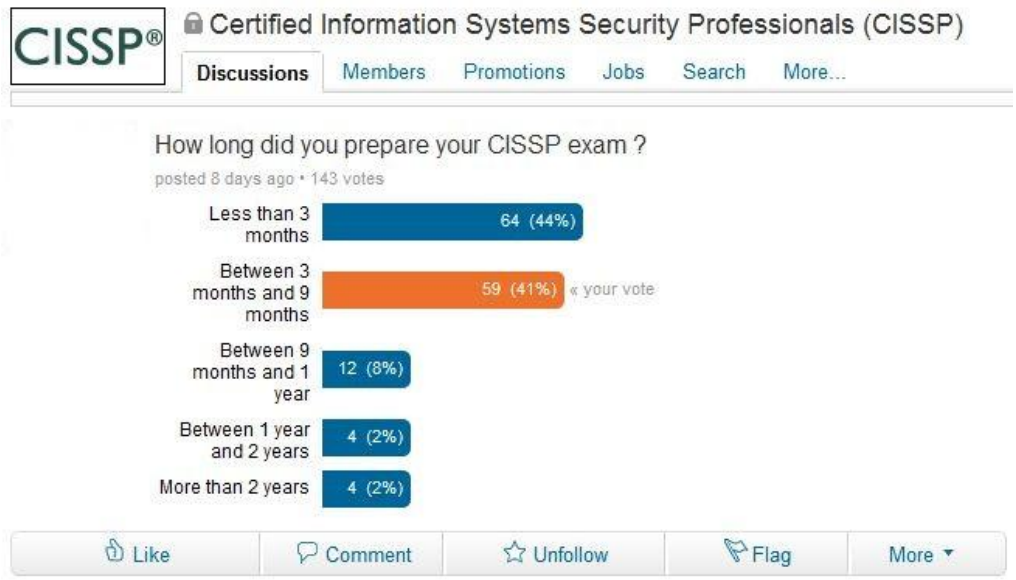
למה צריך לתכנן מראש?

כפי שציינתי בתחילת הכתבה, חשוב להבין שנדרשת השקעה בכל אחד מהתחומים. ישנם תחומים גדולים מבחינת כמות החומר, ישנם תחומים קשים ללימוד בגלל איכות החומר וישנם אפילו תחומים קלים וקצרים יחסית. כמו כן, המבחן אינו שוויוני וניתן לזהות תחומים חשובים יותר וחשובים פחות מבחינת כמות השאלות ומבחינת איכות השאלות (רמת קושי וחישוב הציון).

מכאן, ניתן לנהל את הסיכונים שלנו (לימוד 100% של כל החומר אינו מעשי) ולהשקיע יותר זמן ותרגול בתחומים החשובים שביניהם. כמה זמן לוקח למועמד לסיים ללמוד תחום מסויים? אין תשובה חד משמעית לשאלה. ברור שאם המועמד עובד בתחום של קריפטוגרפיה יהיה לו מאוד פשוט ללמוד את התחום למבחן.

כמה זמן ללמוד?

שאלה מאוד אישית, התשובה העיקר תלויה בשלושה פרמטרים: מה הידע של המועמד (רקע), כמה הוא יכול לשקיע (יש הבדל בין 4 שעות בשבוע לבין 4 שעות ביום) ורמת המשמעת העצמית של המועמד. פרסמתי סקר קטן בקבוצה הרשמית של מוסמכי CISSP ברשת Linkedin כדי לנסות להבין כמה זמן בממוצע מועמד השקיע להכנת המבחן. ניתן לראות את התוצאות לאחר שמונה ימים (חשוב לציין שהמדגם אינו מייצג, מדובר בפחות מ-150 אנשים):



אפשר לראות שמעל 50% מהנשאלים מדווחים על תקופת הכנה של לפחות שלושה חודשים. אין ספק שלתכנן לו"ז מראש לשלושה, שישה או עשרה חודשים הינה משימה מורכבת מכיוון שאנשים עובדים (לפעמים יש לחץ בעבודה), חיים במסגרת (זוגיות, משפחה, חברים) ולא תמיד מכירים את כל הפקטורים

(בלת"מים כגון מילואים, הריון ועוד). אישית, למדתי בערך חמישה חודשים בצורה יחסית אינטנסיבית (בין שעתיים לארבע שעות בערב ברוב ימי השבוע + 8 שעות בשישי/שבת).

כדי להיות מסוגלים לדעת כמה זמן אתם צריכים, אני מציע לקחת אחד מספרי הלימוד ולעבור עליו באופן כללי. בנוסף, מומלץ לעשות סימולציה כדי להבין מהם התחומים החלשים שלכם ומהו היקף הלימודים הנדרש בכל אחד מהתחומים.

מה ללמוד?

- **האם השאלות במבחן מחולקות בצורה שווה בין כל עשרת התחומים?** לא, ויש אפילו משקל משתנה בין השאלות אבל אין דרך לדעת כמה שווה שאלה ביחס לאחרת
- **האם ישנם תחומים שניתן לוותר עליהם?** בגדול, כן.
- **האם ישנם תחומים שאסור לוותר עליהם?** בהחלט.
- **מה הדירוג של התחומים לפי חשיבותם?** זאת שאלה שלא ניתן לענות עליה בצורה חד משמעית וזאת משתי סיבות: ארגון ISC2 אינו מפרסם נתונים ולא מדרג את התחומים. בנוסף לכך, קשה להגיע להסכמה ברורה מכוון שכל דירוג יהיה מבוסס על הדעה הסובייקטיבית של אנשים שעברו את המבחן (ברוב המקרים רק פעם אחת או שתיים).

אישית, אני מאמין שאסור לוותר על מספר תחומים. במידה והמועמד נכשל באחד מהם במהלך המבחן, יש סבירות גבוהה שהוא ייכשל במבחן כולו. תנו דגש לתחומים הבאים:

- Access Control
- Telecommunications
- Information Security Governance and Risk Management
- Software Development Security
- Security Architecture and Design
- Business Continuity and Disaster Recovery Planning

אני ממליץ לגלוש בפורומים ואתרים השונים, ישנם וויכוחים לגבי מהם התחומים החשובים ביותר.

פקטורים נוספים?

אם לאחר שבוע/שבועיים נכנסתם לחומר ויש לכם צפי כללי - מצבכם מעולה. חשוב להתאים את הצפי למציאות ככל האפשר. תתייחסו לפקטורים הבאים.

העבודה: אם החלטתם ללמוד כל יום שעתיים לאחר סיום יום העבודה, חשוב לוודא שלא מתוכננים פרויקטים חשובים ורגישים בחודשים הקרובים (לפחות ממה שאפשר לחזות). במידה וידוע לכם מראש על לחץ מיוחד בחודשים הקרובים, תדחו את תחילת הלימודים. עדיף להמתין ולשמור על רצף הלימודים. אני גם מציע לנסות לקבל תמיכה מהבוס. הבוס יבין שאתם מנסים להשקיע בעצמכם והוא ירוויח מזה בסוף מבחינה מקצועית. יתכן והוא יהיה יותר סובלני בתקופת הלימודים ובעיקר בתקופת המבחן. למה לא

לבקש ממנו עזרה בהכנה? לפעמים אפשר לקבל עזרה כספית (לקורס הכנה או למבחן עצמו), שווה לשאול.

הקרובים/המשפחה: לפי דעתי, ללא ספק הפקטור החשוב ביותר. אם אתם חיים בזוגיות, חשוב לדבר עם בן/בת הזוג ולהבין שמדובר בפרויקט משותף. תצרכו הרבה זמן ללמוד וקשה מאוד ללמוד כשבן/בת הזוג לוחץ לצאת לבילוים או לחופשה. כדאי לנסות לתכן תקופה בה תקבלו תמיכה נפשית והבנה. בזמן הלימודים שלי, אשתי אפילו לחצה עליי כמה פעמים כשהייאוש דפק בדלת. אם יש לכם ילדים, כדאי למצוא סידור מראש ברמה השבועית ושנתית. אני שוב אומר וחוזר, מדובר בפקטור הכי חשוב, כי בלי תמיכה, זה פשוט לא יקרה.

שיטת הלימוד: מאוד חשוב להבין מהי מסגרת הלימודים. קצב ההתקדמות יהיה שונה אם החלטתם ללמוד דרך קורס הכנה או לבד או בקבוצה קטנה. אישית, נפגשתי פעם בשבוע עם חבר שגם למד למבחן, פתרנו שאלות במהלך שעתיים/שלוש, רשמנו לעצמנו הערות וחזרנו ללמוד כל אחד לבד בבית.

הלחץ/הפחד: קשה להתמודד עם הקושי הפסיכולוגי אבל אפשר להשפיע עליו ולנסות לנצל אותו לטובת המטרה. כל אחד יכול להמציא את השיטה שלו, אני אפרט את השיטה שלי. קודם כל תכנון יום המבחן: החלטתי להיבחן באפריל וזה הפך לתאריך יעד. הרבה יותר קל להחליט כמה זמן להשקיע בסה"כ ובכל תחום כשיש תאריך יעד. דבר נוסף, דיווחתי על המטרה שלי (לעבור את המבחן) לאנשים הקרובים אליי (חברים מהעבודה, בוס, משפחה קרובה, חברים קרובים). מהרגע שהצהרתי על הכוונות שלי, שאלו אותי איך מתקדמים הלימודים... סוג של לחץ שדחף אותי להמשיך ללמוד במיוחד כשרציתי להפסיק.

לו"ז סופי:

הגיע הזמן לדבר על מספרים. כדאי לרשום את הלו"ז ולוודא שאתם עומדים בתכנון כל שבוע. אציג לכם את לוח הזמנים שלי לחודשים האחרוניים:

MONTH	WEEK	Start	End	DOMAIN
נובמבר	1	18/11/2011	24/11/2011	Security Architecture & Design - Book
	2	25/11/2011	01/12/2011	Security Architecture & Design - Book & Practice
דצמבר	3	02/12/2011	08/12/2011	BCP and DR
	4	09/12/2011	15/12/2011	Legal, Regulations, Investigations and Compliance
	5	16/12/2011	22/12/2011	Operations Security - Book
	6	23/12/2011	29/12/2011	Operations Security - Book & Practice
ינואר	7	30/12/2011	05/01/2012	Cryptography - Book
	8	06/01/2012	12/01/2012	Cryptography - Book & Practice
	9	13/01/2012	19/01/2012	Access Control - Book
	10	20/01/2012	26/01/2012	Access Control - Book & Practice
פברואר	11	27/01/2012	02/02/2012	Telecommunications and Network Security - Book
	12	03/02/2012	09/02/2012	Telecommunications and Network Security - Book & Practice
	13	10/02/2012	16/02/2012	Physical and Environmental Security
	14	17/02/2012	23/02/2012	Information Security and Risk Management - Book
	15	24/02/2012	01/03/2012	Information Security and Risk Management - Book & Practice
מרץ	16	02/03/2012	08/03/2012	Application and Systems Development - Book
	17	09/03/2012	15/03/2012	Application and Systems Development - Book & Practice
	18	16/03/2012	22/03/2012	Overall + Practice
	19	23/03/2012	29/03/2012	Overall + Practice
	20	30/03/2012	31/03/2012	Overall + Practice
אפריל		01/04/2012		**EXAM**

קביעת לוח זמנים הינה פעולה קריטית בפרויקט ארוך כמו הכנה למבחן ה-CISSP. חשוב להבין שחשיבה נכונה בשלב זה תגרום להצלחה או לכישלון במבחן.

השלב הקשה ביותר: להתחיל

ההורים שלי לימדו אותי שבחיים אין מתנות חינם ושהפחד לא מוריד את הסכנה. אני חייב לצטט את הקטע המפורסם של הסרט "מבצע סבתא":

סרג'יו: "הנכד שלי כבר חודש לא יורד את השתי דקות ב-100 מטר."

קרמבו: "יש רק דרך אחת לשחות 100 מטר."

סרג'יו: "קרמבו, תן איזה טיפ של אלופים."

קרמבו: "אתה מתחיל הכי מהר שלך, ולאט לאט אתה מגביר."

אין דרך אחרת להגיד: תתחילו ללמוד ואל תחפשו תירוצים. תעמדו בלוח הזמנים שקבעתם (הרבה אנשים טובים ויתרו על המבחן כי איבדו את התכנון בדרך).

מאיפה להתחיל?

לפני הכל, קחו את הזמן לשמוע את ההרצאה של Clement Dupuis שעובר בגדול על כל התחומים ועל המבחן עצמו (המצגת לא כל כך חדשה אבל עדיין מאוד רלוונטית).

אני ממליץ להתחיל עם הפרקים הקשים. למה קודם הפרקים הקשים? כי ככל שהזמן חולף ומתקרבים למועד המבחן, עדיף פחות "להתאמץ" בהבנה ויותר בחזרות ותרגולים. בנוסף, אם תתחילו עם הנושאים הקשים, יהיה לכם יותר זמן לעבור שוב ושוב עליהם כדי להבין, להפנים ולזכור.

מהם הפרקים הקשים? הזכרתי מוקדם יותר שחלק מהתחומים חשובים יותר מאחרים במבחן עצמו (יותר שאלות). אם חלק מהם חדשים לחלוטין למועמד. רמת הקושי עולה ושם צריך להתחיל. באופן ככלי, מקובל להגדיר את התחומים הבאים כקשים גם בגלל המורכבות ו/או היקף החומר:

- Cryptography
- Software Development Security
- Telecommunications and Network Security

שימו לב: רמת הקושי של כל תחום משתנה בהתאם לרקע של המועמד.

אם אתם לומדים במסגרת כלשהי (קורס, קבוצת לימוד, סדנא): מומלץ מאוד ללמוד בהתאם לנושאים הנלמדים בזמן אמת.

אני לא מבין את החומר, מה עושים?

לא להבין מושגים הינה תופעה ידועה וטבעית. לא צריך להילחץ. אם אתם לומדים במסגרת כלשהי (קורס, סדנא, קבוצה), תתייעצו עם אחרים/מרצה. אם אתם לומדים לבד: תקראו מספר פעמים את החומר, תנסו למצוא הסברים מקבילים (Google, Wikipedia) ובסוף תבקשו עזרה בפורומים מקצועיים (אישית אני ממליץ על קבוצות לימוד בלינקדין כאן או כאן ובפורום של אתר CCCure).

אני מבין אבל לא זוכר, מה עושים?

זאת אחת הבעיות הגדולות בלימוד החומר. איך לזכור את החומר בצורה נכונה (לא מספיק לדעת את החומר, צריך גם לזכור את הסדר ופרטים קטנים נוספים)? חייבים לעבור על החומר שוב ושוב אבל יש קיצורי דרך. אפשר להשתמש בשיטות "ממו טכניות".

דוגמא א': מודל OSI:

אני עובד בתחום התשתיות כבר מספר שנים ואני מכיר את מודל השכבות OSI אבל עד המבחן לא הייתי מסוגל לזכור את הסדר של השכבות בעל פה. אחת השיטות היא לזכור את המשפט "All People Seem To Need Data Processing" ואתם זוכים את הסדר לפי האות הראשונה של כל מילה.

- **A** - Application
- **P** - Presentation
- **S** - Session
- **T** - Transport
- **N** - Network
- **D** - Data Link
- **P** - Physical

דוגמא ב': סוגי אש:

מי זוכר את סוגי האש (A,B,C,D)? תזכרו רק את שם הפרטי של Clement Dupuis (של המצגת) וקל יותר לזכור את סוגי האש והמקור שלהם.

CLEMent

- **A** = **C** - Common Combustible
- **B** = **L** - Liquid Fire
- **C** = **E** - Electric Fire
- **D** = **M** - Methals

כל אחד יכול לבנות לעצמו את המילים/משפטים שיעזרו לו לזכור אבל מומלץ ללמוד מהניסיון של אחרים. גשו לפורום של CCCURE ותגלו פוסט שמרכז את הסודות של כולם (קישור ישיר לפוסט).

סוד ההצלחה: תרגול, תרגול ועוד תרגול

המבחן מכיל 20 שאלות וצריך לענות עליהם תוך 6 שעות. מדובר במרתון פסיכולוגי מעייף כי לא פשוט לשבת כל כך הרבה זמן בריכוז מלא. רוב השאלות מורכבות גם למי ששולט בחומר. הדרך הטובה לעבור את המכשולים היא להתכונן "לאופי" המבחן ולהפחית את הלחץ ככל שניתן.

בפרק הקודם, הצגתי את התכנון שלי ואפשר לראות שהשבועיים האחרונים הוקדשו לחזרות ולתרגול. אציין שתיאמתי שבוע חופש מהעבודה לפני המבחן וזה מאוד עזר כדי ללמוד "בשקט". התחלתי את החזרות עם שתי סימולציות של 100 שאלות (כל אחת) ביום. לאחר מכן, עליתי ל-200 ול-250 שאלות (סימולציה אחת ביום). מדדתי זמן לכל הסימולציות.

שימו לב: הנקודה החשובה היא לא לסיים את הסימולציה בזמן (בדרך כלל הייתי מסיים 100 שאלות תוך 50 דקות) אלה להתרגל לאופי המבחן ולסבולת הנדרשת (לשמור על הריכוז לאורך הזמן, לנסות לפתור מקסימום שאלות במינימום זמן, לא לבזבז זמן על השאלות הקשות ועוד).

המשימה הקשה והמתישה היא לא הסימולציה עצמה אלה לעבור לאחר מכן על השאלות שוב ולנסות להבין למה התשובה נכונה או שגויה. תהליך זה יאפשר מיקוד בחומר הבעייתי וחיזוק הביטחון העצמי. חזרתי פרטנית על 70/80% מהשאלות (דילגתי על השאלות הקלות).

האם אני מוכן?

שאלת מיליון הדולר (או מאות הדולרים ליותר דיוק כי זה מה שיעלה לכם רישום למבחן חוזר). מקובל להגדיר את רמת המוכנות בהתאם לתוצאות בסימולאציות.

המספרים מאוד יחסיים וזאת משתי סיבות:

- כל מערכת סימולציה בעלת רמת קושי שונה. מומלץ להשוות מה שניתן להשוות, אם קיבלתם 80% הצלחה בסימולציות AIO (של Shon Harris) או 75% הצלחה במבחני CCCure.org, אתם מוכנים. לגבי הסימולציות של המכללות, תתייעצו עם המרצה.

- מכיוון שסך השאלות לתרגול מוגבל, יש סבירות גבוהה שתעברו שוב ושוב על אותן השאלות ותענו בצורה אוטומטית כי אתם מכירים כבר את התשובה (לא תמיד במודע).

קשה לי לאמין שניתן לעבור את המבחן בלי לתרגל **1000/1500 שאלות מינימום** (אישית תרגלתי מעל 2000).

אני ממליץ בחום להוריד מהרשת מסמכי CRAMS שונים (מסמכים שמרכזים את המושגים החשובים) ולבדוק שאתם מכירים אותם. ניתן לגשת לכמה דוגמאות בדף ה-Cheat Sheet בבלוג שלי.

אסטרטגיה:

יש שיטות שונות להתמודד עם השאלות, לא משנה כל כך מהי השיטה שתבחרו, העיקר שתקבעו אסטרטגיה ותעמדו בה. אסטרטגיה ברורה גם תעלה את רמת הביטחון העצמי.

להלן חוקי הברזל שהגדרתי לעצמי (על סמך ניסיון של האחרים ועל סמך הניסויים בסימולציות):

- תמיד לקרוא את השאלות פעמיים ולהדגיש מילות מפתח: לשים לב למילות המפתח של השאלה כגון NOT, NEVER, BEST, ALWAYS... (אם השאלה מורכבת במיוחד, לסמן את השאלה לטיפול מאוחר יותר).
- לנסות לזהות את התחום (Domain) הקשור לשאלה: לדוגמא, אם השאלה מתייחסת לתחום Operations Security, תצפו לתשובה בהתאם.
- להתחיל לקרוא את התשובות מהסוף אל ההתחלה (קודם לקרוא את התשובה d., את התשובה c וכו).
- קודם כל, לסמן את התשובות הלא נכונות: אישית, הפכתי את השאלות (תשאלו את עצמכם את השאלה בצורה הפוכה).
- במידה ולא מצאתם את התשובה מיד (תוך 20-30 שניות), לסמן את השאלה לטיפול בסוף - יתכן והתשובה תהיה ברורה בקריאה השנייה.

ואת החוק החשוב ביותר...

- לאחר סימון תשובה, אין לשנות דעה - הניסיון מלמד שהאינסטינקט הראשוני שלכם בדרך כלל נכון. יש סבירות גבוהה ששינוי יביא לטעות (שלא לדבר על בזבוז בזמן).

אין הבדל בניקוד בין תשובה שגויה לבין שאלה שלא נענתה. חשוב לוודא שאתם עונים על כל השאלות כי גם אם אתם לא מכירים את התשובה, יש לכם סבירות של 25% לענות נכון (יותר טוב מכלום).

טיפים של הרגע האחרון

הרבה מבקשים "טיפ אחרון" בערב המבחן, קבלו שניים:

קודם כל, תרגעו! לא בדיוק מפתיע, אבל כל כך נכון. 24 שעות לפני המבחן, אל תתעסקו בחומר. תנסו להירגע, לכו לים, לשחק כדורסל או צאו לסרט. תנסו לישון טוב ביומיים האחרונים ותקפידו על אוכל קליל.

ניהול הזמן: עוד לפני יום המבחן, תנסו לקבוע שיטה "לניהול זמן" ברורה ותעמדו בה. עוד משהו קטן שיעלה לכם את הביטחון העצמי. אישית, חילקתי את המבחן ל-5 חלקים:

- **חלק 1 (שעה): 100 השאלות הראשונות** - לענות על מקסימום שאלות במינימום זמן. להשאיר את השאלות הקשות בצד.
- **חלק 2 (שעה): 100 השאלות הבאות** - כנ"ל.
- **חלק 3 (חצי שעה): 50 השאלות האחרונות** - כנ"ל.
- **חלק 4 (שעה-שעה וחצי):** להתמקד בשאלות הקשות שהשארתם בצד.
- **חלק 5 (שעה):** סיבוב אחרון על השאלות שסומנו.

כמובן, מומלץ לצאת להפסקה לפחות פעם אחת. אישית, יצאתי שלוש פעמים להפסקת קצרות. שימו לב: הגדרתי מראש יותר זמן מהנדרש וזכיתי בזמן "ספייר" שהרגיע אותי. אנשים שמתחילים לענות ישיר על 250 שאלות לא תמיד מסוגלים לנהל את הזמן בצורה ריאלית. לחלק את המבחן לחלקים קטנים מקטין את הסיכוי שיחסר לכם זמן בסוף.

מה להביא ביום המבחן?

שבועיים לפני המבחן שלי, החלטתי לעשות Shopping מיוחד. לא חייבים לקנות הכל מחדש אבל להלן רשימה של פריטים שמומלץ להביא ביום הדין (חלקם חובה):

- **מכתב ההזמנה מודפס: שלא תעזו לשכוח!**
- **דרכון (או ת"ז) + מסמך מזהה נוסף** (רישיון נהיגה לדוגמא).
- **ז'קט/מעיל קל** (למקרה של מתקפת מזגנים).

- **מילון (שתי שפות):** ללא ציורים והסברים, רק תרגום מילה במילה. אישית, אני ממליץ להביא לפחות שני סוגים כי מרכז המבחן יכול לפסול כל סוג כלא מתאים (אין רשימת מילונים מורשים, ההחלטה סובייקטיבית לחלוטין ואתם לא רוצים להתחיל להתווכח ביום המבחן).

- **אטמי אוזניים:** כשהרכבת תעבור ליד הכיתה או כשהמועמד הצמוד יתחיל לאכול ירוקות שורש (מקרה אמיתי) תצרכו להתנתק מהרעש. ממליץ על אטמים מסיליקון, הם מאוד נוחים. תקבלו אטמים חד פעמים אבל אישית, אני לא חושב שהם נוחים.

- **Crams מודפסים**. ניתן לעבור על החומר בקלילות עד לתחילת המבחן.

- **נשנושים "חכמים":** כל אחד בהתאם לבטן שלו. אם זאת, תשתדלו לא להביא דברים "מלכלכים" (קוביות שוקולד לדוגמא). מומלץ להביא חטיפי אנרגיה.

- **שתיה** - תביאו בקבוק מים.

רגע האמת:

המבחן מתקיים בכיתות מחשוב במרכז PEARSON הנמצא רמת גן (דרך בן גוריון 2 - קישור למפה), צריך להגיע מוקדם (מינימום חצי שעה לפני תחילת המבחן, עדיף להקדים עוד קצת), אני ממליץ "לסייר" מראש כדי להימנע מטעות של הרגע האחרון.

בתקופתי, המבחן היה PBT (מבוסס כתיבה על נייר) אבל היום המבחן הינו ממוחשב (Computer Based Test - CBT). תוצאת המבחן תתקבל מיד עם סיומו.

במידה ועברתם - מזל טוב! אפשר לחזור הביתה ולהתחיל את תהליך ה-Endorsemet. אגב, אין ציונים למי שעובר. אצל ISC2, כל העוברים שווים.

במידה ונכשלתם - לא נורא! זה קורה להרבה מועמדים לעבור בפעם השנייה (או שלישית). קחו כמה ימים של חופש מהלימודים ותחזרו ללמוד. מועמד שנכשל מקבל את הציון שלו ואת הרשימה של התחומים מדורגת לפי הצלחתם במבחן. תחזרו ללמוד ותנו דגש על התחומים החלשים

לכולם - תאספו את הציוד שלכם, סעו למקום רגוע (הים מקום נהדר), נשנשו משהו וחזרו הביתה לישון (לאחר המבחן אתם תהיו מרוקנים נפשית ורק שינה יכולה לעזור).

סיכום

הסמכת ה-CISSP הינה התעודה הידועה בארץ ובעולם בתחום אבטחת המידע. בניגוד להסמכות אחרות, לא ניתן "לזייף" את רמת הידע הנדרש ולכן ההסמכה נחשבת כאיכותית. על מנת לעבור את המבחן, יש להתכונן בהתאם ומאמר זה מהווה בסיס חשיבה לתהליך ההכנה.

על המחבר

דודו ברודה, מנהל אקדמי של קורסי הגנה (CISO, CISSP ועוד) ויועץ אבטחת מידע בחברת See-Security. בעל ניסיון רב בתחום, בעבר ניהל את תשתיות המחשוב והתקשורת במשרד ממשלתי.

המאמר פורסם במקור בבלוג של דודו כסדרת כתבות במטרה לעזור לכל המעוניין להתכונן ולעבור את מבחן ה-CISSP ולהתקדם בתחום. סדרת הכתבות מתעדכנת בבלוג על בסיס חודשי.