חוות דעת מומחה

אני החתום מטה, אור דונקלמן, ת.ז. 040343329, נתבקשתי על ידי התנועה לחופש המידע לתת חוות דעת מומחה בנושא השפעות של חשיפת קוד מקור על אבטחת המידע ובמיוחד בהקשר של מחשבון מסוים של המוסד לביטוח לאומי. כמו-כן, התבקשתי להגיב למספר טענות טכניות שהועלו בחוות דעת שצורפה כנספח לכתב התשובה של המוסד לביטוח לאומי.

אני מצהיר בזאת כי ידוע לי היטב, שלעניין הוראות החוק הפלילי בדבר עדות שקר בשבועה בבית המשפט, דין חוות דעתי זו כשהיא חתומה על ידי כדין עדות בשבועה שנתתי בבית המשפט.

רקע אקדמי ומקצועי

אני משמש כחבר סגל בדרגת פרופסור מן המניין (עם קביעות) בחוג למדעי המחשב באוניברסיטת חיפה. בעל תואר שלישי במסלול הישיר (Ph.D.) מהפקולטה למדעי המחשב בטכניון, ותואר ראשון בהצטיינות יתירה (B.A. summa cum laude) מהפקולטה למדעי המחשב בטכניון. פרסמתי כ-90 מאמרים בכנסים בינלאומיים ומעל ל-35 מאמרים בירחונים מדעיים, הכל כמפורט בנספח א'.

כחלק מתחומי המחקר שלי, שימשתי כאחד ממנהלי המרכז חקר סייבר, משפט ומדיניות באוניברסיטת חיפה, וכן כמנהל תת המרכז לחקר הביומטריה ויישומיה הפועל במרכז הנ"ל, הייתי חבר במרכז הירושי פוג'יוארה לאבטחת סייבר שבטכניון, שימשתי כחבר הועד המנהל של הארגון הקריפטוגרפי הבינלאומי (IACR), ואני אחד ממייסדי עמותת פרטיות ישראל. בנוסף לאלה, אני משמש כאחד מנציגי ישראל (כנציג מכון התקנים הישראלי) בועדות התקינה בתחום הקריפטוגרפיה ואבטחת המידע של ארגון התקינה הבינלאומי ISO.

תחומי המחקר וההוראה העיקריים שלי הם:

- אבטחת מידע (סייבר) – שימשתי כמרצה בקורס הטכניוני עוד ב-2003 (עד 2006, שיצאתי לחו"ל ללימודי פוסט-דוקטורט), ומאז קבלתי כחבר סגל באוניברסיטת חיפה ב2011. מעבר להוראה, צברתי ניסיון פרקטי בתחום זה במערכות משובצות מחשב במספר מקומות.
- חוקר קריפטוגרפיה (הצפנה) עם דגש על צפני מפתח משותף. אני מתמחה בפיתוח שיטות תקיפה לצפנים אלה, וכן בבדיקת חוזקם של צפני מפתח משותף ונגזרותיהם.
- פרטיות ואנונימיות – בעיקר התקפות כנגד שיטות הגנה שנועדו להגן על פרטיות המשתמשים.
- ביומטריה – שימוש בזיהוי ביומטרי, כיצד להגן על פרטיות של מידע ביומטרי ותקיפת מערכות ביומטריות.

פרטים נוספים לגבי ניסיוני, השכלתי, כולל רשימת פרסומים, האוניברסיטאות בהן לימדתי ולמדתי ועוד, מפורט בנספח א'.

פרק I – הרקע לחוות הדעת

1. כחלק מההליך המשפטי בו ניתנת חוות דעת זו, ביקשה התנועה לחופש המידע מהמוסד לביטוח לאומי לחשוף קוד מקור של מחשבון מיצוי זכויות וטבלת אקסל הנמצאת באיפיון התוכנה.
2. המחשבון הורד מאתר המוסד לביטוח הלאומי, ולכן לא ניתן לבחון אותו בכללותו. עם זאת, בחנתי הן את מסמכי האיפיון של המחשבון, והן את המחשבונים האחרים הפועלים באתר המוסד לביטוח לאומי לצורך חוות דעתי זו.
3. כתב התשובה המתוקן מיום 20.6.24 מעלה שתי טענות עיקריות – הראשונה היא שקוד מקור איננו מידע במובנו החוקי וכי חשיפת קוד המקור תפגע באבטחת המידע של המוסד לביטוח לאומי (וכתוצאה מכך בפרטיותם של תושבי ישראל).
4. קראתי את נספח 1 של כתב התשובה המתוקן לעומקו, ואני סבור שטענותיו בתחום אבטחת המידע אינן עולות בקנה אחד עם הידע המדעי והטכולוגי בתחום אבטחת המידע, והוא איננו עולה בקנה אחד עם ה-best practices הנהוגים בתחום.
5. לפיכך, עיקר הפגיעות הנגזרות, אף הן אינן עולות בקנה אחד עם הידע המדעי והטכנולוגי בתחום, ובמיוחד בהקשר של המחשבון המדובר.
6. מטרת חוות דעת זו היא להסביר את קביעתי, על סמך ניסיוני ומומחיותי, וכן להעמיד על דיוקן מספר טענות שהועלו בחוות הדעת המצורפת לכתב התשובה המעודכן.

פרק II – תמצית חוות הדעת

7. חוות הדעת בנספח א' קושרת בין סודיות קוד לבין אבטחת מידע מוגברת. זוהי טענה שהוכחה חזור והוכח כלא נכונה. יתר על כן, מדינות רבות נוקטות בהעדפה ברורה לתוכנות קוד פתוח לשימושיהן, מכיוון שהן מספקות (בין היתר) אבטחה גבוהה יותר.
8. חשיפת קוד מקור מאפשרת לציבור להציע שיפורים ותיקונים לקוד, הן בתחום הפונקציונאלי (כלומר, תיקון באגים) והן בתחום אבטחת המידע (ובכך לייצר קוד בטוח יותר).
9. נהלי אבטחת מידע בתחומים קריטיים אינם פוסלים (ולעיתים אף מעודדים) שימוש בקוד פתוח. כלומר, גם כשיסתיים התהליך של הגדרת המוסד לביטוח לאומי כתשתית מידע קריטית של מדינת ישראל, אין מניעה בחשיפת קוד של המחשבון בליבת הדיון, מטעמי אבטחת מידע.
10. בדקתי מספר מחשבונים באתר המוסד לביטוח לאומי – אף אחד מן המחשבונים המוצגים איננו "מושך" מידע משרתי המוסד לביטוח לאומי (כלומר, כל פרטי המחשבונים מסופקים על ידי המשתמש). לפיכך, אף אחד מהמחשבונים, ולפיכך גם המחשבון נשוא העתירה איננו מהווה "נקודת חולשה" דרכה ניתן לפגוע באבטחת המידע של המוסד לביטוח לאומי (ולכן גם בפרטיות המידע של משתמשיו).
11. אחדד, מחשבון שאיננו מסתמך על מידע פנימי הנמצא במערכות המוסד לביטוח לאומי, ומסתמך אך ורק על מידע המגיע מן המשתמש, לא אמור להכיל ממשקים אל תוך מערכות המוסד לביטוח לאומי, ולכן איננו מהווה נקודת תורפה בנוגע למערכות תפעוליות ו/או אתר האינטרנט של המוסד לביטוח לאומי.
12. כמו-כן, טענות על היכולת להסיק מסגנון כתיבת הקוד של מחשבון מסוים לחורי אבטחה הקיימים במערכת אינן מעוגנות בספרות המחקרית ואינן משמשות בתהליכי מציאת חורי אבטחה ככל שידיעתי משגת.
13. כלומר, עמדתי החד משמעית היא שחשיפת קוד המקור של מחשבון זה או אחר, המצוי באתר המוסד לביטוח לאומי, ואשר איננו מקושר למאגרי המידע של המוסד (כלומר לא מקבל מידע מתוך מערכות המחשב של המוסד לביטוח לאומי), איננה מגדילה את סיכוני הסייבר של המוסד לביטוח לאומי.
14. עמדתי אף מתחזקת לנוכח העובדה שאתר המחשבונים של המוסד לביטוח לאומי חושף מידע פרטי על משתמשי האתר בפני שרתי חברת גוגל. כדי לוודא שגם המחשבונים הקיימים (בעבר, בהווה ובעתיד), אינם חושפים מידע נוסף, יש לבדוק את קוד המקור שלהם.

פרק III – מהי תוכנה, מהו קוד מקור, מהו קוד מקור פתוח וסגור

15. ראשית, אתחיל את חוות דעתי בהסבר קצר מהי תוכנת מחשב, מהו קוד המקור שלה, וההבדל בין קוד מקור סגור לעומת קוד מקור פתוח.
16. תוכנת מחשב הינה רצף פקודות, בשפת מכונה הגורמת למחשב לבצע חישובים ופעולות מסוימות (לדוגמא, חיבור של מספרים, הצגה של הודעה על המסך, התחברות למאגר מידע ועוד).
17. שפת המכונה מטבעה ברורה למכונה, והיא מורכבת מפקודות (המקבילה למילים/משפטים) הכתובים בצורה שהמחשב יכול להבין אותה ביעילות רבה. באותה העת, כמעט כל המתכנתים אינם יכולים לקרוא ביעילות את שפת המכונה, ובוודאי לכתוב בה את הפקודות למכונה.
18. במקום זאת, משתמש המתכנת בשפת תכנות – שפה שמתווכת בין הרעיונות הבסיסיים שיש לנו בנוגע למחשב (לדוגמא, אפשר לחשוב על משחק מחשב כמו טטריס, שבו יש עקרונות שאדם חשב עליהם), לבין שפת המכונה.
19. המתכנת אם כך, לוקח את הרעיונות, וממשש אותם תוך שימוש בשפת התכנות. כלומר, הוא מפרק את הרעיונות הגדולים לצעדים קטנים יותר, הנכתבים בשפת תכנות שהיא קרובה יותר לשפת מכונה מבחינת המבנה והתוכן שלה, אך ניתנים לקריאה אנושית. לדוגמא, בשפת התכנות Python, כדי להדפיס למסך את המילים "Hello World", יכתוב המתכנת בשפת התכנות את הפקודה ("print("Hello World. תוכנה, אם כך, היא אוסף פקודות בשפת תוכנה שכתב המתכנת.
20. לאחר כתיבת התוכנה, היא עוברת תהליך של הידור (קומפילציה בלעז) או של אינטרפרטציה – שבו התוכנה הופכת לפקודות שמחשב מסוגל להבין ולבצע.
21. התוכנה שנכתבה היא אם כך קוד המקור.
22. קריאת קוד המקור מאפשרת לבדוק את נכונותו (לדוגמא, לוודא שהוא מחשב את מה שהוא אמור לחשב), לזהות האם קיימות בו שגיאות תכנות (כלומר, באגים), ואפילו לזהות בו חורי אבטחה.
23. יש לציין כי אפשר לבצע את הפעולות הנ"ל גם מהתבוננות בתוכנת המחשב (בתהליך הקרוי הנדסה לאחור, או reverse engineering), אך הוא מסובך יותר ודורש מומחיות גדולה יותר.
24. לכן בעולם נהוגות בגדול שתי גישות בנוגע לקוד המקור – הראשונה דוגלת בשמירת קוד המקור לא נגיש לקהל הרחב (גישה הידועה לרוב כקוד סגור) והשניה דוגלת דווקא בפרסום קוד המקור (גישה המכונה – קוד פתוח, אם כי יש בה מספר זרמים בהתאם לתפישות שונות בהקשרי קניין רוחני).
25. לא מעט מהתוכנות הנמצאות בשימוש יומיומי היום, נכתבו ופותחו עם קוד פתוח (לדוגמא, מערכת ההפעלה אנדרואיד, המפעילה את מרבית הטלפונים החכמים בארץ ובעולם, או דפדפן כרום של חברת גוגל המתבסס על פרויקט הקוד הפתוח chromium). מרבית חברות התוכנה הגדולות בעולם תומכות בפרויקטי קוד פתוח שונים (ביניהן חברת מיקרוסופט, אפל, גוגל, IBM ועוד).

פרק IV – האם קוד פתוח וזמין פוגע בבטיחות מערכות?

26. אחת מטענות הבסיס של חוות הדעת בכתב התשובה המתוקן היא כי פרסום קוד, כלומר הפיכתו לפומבי פוגעת באבטחת המערכת.
27. טענה זו עשויה להיות נכונה בהקשרים של קוד במערכות אשר השגת הקוד היא מסובכת מאוד ו/או הוא מיועד לסביבות הרצה מאוד מיוחדות (לדוגמא, קוד המשמש במערכת צנטריפוגות להעשרת אורניום המיועד לרוץ על בקרים מסוימים של חברת סימנס).
28. עם זאת, בהקשרים של קוד כללי הרץ על מחשבים רגילים, הטענה כי קוד מקור פתוח מהווה בעיית אבטחת מידע, לא נסמכת על המלצות גופים מקצועיים כגון מכון התקינה הטכנולוגי האמריקאי (US National Institute of Standards and Technology) או ארגון ה- OWASP (open worldwide application security project). גם תקני אבטחת מידע מובילים בעולם, כגון סדרת תקני אבטחת המידע של ארגון התקינה הבינלאומי ISO (International Standardization Organization), הידועה כסדרה 27000 (סדרת תקנים בתחום אבטחת המידע), איננה אוסרת שימוש בקוד פתוח.
29. דוגמא לכך שאין מדובר בטענה מקובלת בתעשיה, אציין כי המדריך לפיתוח קוד בטוח (פרסום 800-218 של מכון התקינה הטכנולוגי האמריקאי) הקרוי Secure Software Development Framework (SSDF) (מהדורה 1.1), מגדיר תהליכים דרושים לאבטחת מידע בסביבות פיתוח המכילות ו/או מסתמכות על קוד פתוח. מכאן, קל להסיק שקיומו של קוד פתוח איננו חולשת אבטחה.
30. כאמור, גם סדרת תקני אבטחת המידע המובילים בעולם (סדרת תקני האבטחה ISO 27000) לא מונעים שימוש בקוד פתוח ומאפשרים שימוש שכזה. אמנם, קריאה "חפוזה" ולא מעמיקה בתקן

אבטחת המידע ISO 27001 מכילה את האמירה (תחת סעיף בקרה A.9.4.5) שהגישה לקוד המקור צריכה להיות restricted. עם זאת, ההבהרה של ההצהרה הנמצאת ב-ISO 27002, מציינת בפירוש כי המטרה היא המנעות משינוי זדוני של התוכנה (כלומר, המנעות ממצב שבו משתמש חיצוני לארגון משנה את הקוד הרץ בארגון). לפיכך, קל לראות כי גם סדרת תקני אבטחת המידע ISO 27000, לא מהווים מניעה לשימוש בקוד פתוח במערכת בטוחה.

31. גם ארגון OWASP הידוע כאמון על קידום מתודות פיתוח בטוחות מפרסם רשימת 10 בעיות אבטחת מידע במהלך פיתוח המכיל קוד פתוח (בדומה לרשימות דומות לפיתוח קוד סגור). רשימת הבעיות הן לפי סדר יורד (נכון לגרסא 0.1 שפורסמה ב-2024) – חורי אבטחה ידועים (כלומר, שימוש בספריות/כלים שידוע שיש בהם חורים), פגיעה הקיימת בספריות הנמצאות בקוד, התקפות המתבססות על שימוש בספריות לא נכונות (עקב שמות קרובים), שימוש בקוד שלא עובר עדכון, שימוש בקוד שעבר זמנו, חוסר מעקב אחרי תלויות של קטעי קוד, בעיות ברישיונות פיתוח, שימוש בתוכנה לא בשלה, שינוי לא מורשה לקוד, ואי זיהוי נכון של תלויות של קטעי קוד. מבלי להכנס לכל אחד ואחד מן הבעיות הללו, אף אחת מהן איננה רלוונטית לקוד שהיה בעברו סגור והוא הופך לפתוח, במיוחד שלפי חוות הדעת שנמסרה (סעיף 28), אף אחת מהבעיות הנ"ל איננה רלוונטית עבורו.

32. אפילו במערכות הצבעה אלקטרוניות, שהן מהמערכות המסובכות ביותר שאפשר להעלות על דעת מבחינת דרישות אבטחת המידע והפרטיות (כפי שאפשר לראות בדו"ח האקדמיה הלאומית למדעים Securing the vote – Protecting American Democracy משנת 2018), אין מניעה להשתמש בקוד פתוח. להפך, המדריך המקיף ביותר בתחום (ה-Voluntary Voting System Guidelines (VVSG) 2.0), מכיל המלצה מפורשת לוידוא חיצוני של קוד המקור של המערכת (סעיף 13.2), כלומר טוען שיש לבצע בדיקה חיצונית של הקוד (כמובן, שהדבר כולל חשיפת קוד בפני גורמים חיצוניים למפתחים) כחלק מהתהליך שמגדיל את אמון הציבור בתוצאות ההצבעה.

33. קוד פתוח מאפשר לוודא שהקוד אכן מבצע את שהוא אמור לבצע. ולכן כאמור, הוא מומלץ במיוחד בהקשרים שבהם יש צורך באמון הציבור בקוד.

34. לדוגמא, קוד המקור של אפליקציות ניטור המגעים במרבית אירופה ששימש בזמן הקורונה (שנגזר מפרוייקט ניטור המגעים DP3T) – היה זמין ופתוח לציבור כדי להגדיל את אמון הציבור שאפליקציות ניטור המגעים אינן אוספות מידע פרטי נוסף מעבר למפורט לציבור. מאידך, אפליקציית הרמזור הישראלית, פותחה בסביבת קוד סגור, אך בעבודה קלה למדי, הצלחנו עמיתיי ואנוכי לבצע הנדסה לאחור לאפליקציה ולמצוא בה מספר בעיות אבטחת מידע (כפי שמתואר לדוגמא, בכתבתו של רן בר-זיק בעיתון הארץ - https://www.haaretz.co.il/captain/software/2021-02-28/ty-article/.premium/0000017f-e03b-d3ff-a7ff-f1bbf9070000).

35. יש לציין כי באף אחד מהמדריכים המוזכרים לעיל (וגם באף מדריך אחר שאני מודע לו), אין המלצה להסתיר קטעי קוד של מתכנת מסוים כדי למנוע מצב של "הנדסה לאחור" של החולשות של אותו מתכנת (כפי שרומזת חוות הדעת במסמל התשובה).

36. יתר על כן, אחת ההמלצות הנפוצות לסטודנטים למדעי המחשב, המעוניינים לעסוק בתחום התכנות, כולל סטודנטים המחפשים עבודה בתחום אבטחת המידע, היא לפרסם קטעי קוד שלהם, ואפילו להשתתף בפרויקטי קוד מקור פתוח, כדרך להראות את עבודתם לעולם (וליצור קשרים). לדוגמא, בכתבה הדנה בצעדים ראשונים בעולם פיתוח התוכנה, מציע מומחה אבטחת המידע רן בר-זיק לייצר לכל פרויקט תוכנה גדול שהמשתמש פיתח לבד (לדוגמא, כחלק מלימודיו) דף פרויקט שמסכם את הקוד שאמור להיות מפורסם באתר דוגמת GitHub. (אתר GitHub, ואתרים דומים לו, מאפשרים למתכנתים המעוניינים בכך לפרסם קטעי קוד).

37. יש לציין כי לא מעט מומחי אבטחת מידע תורמים קוד באופן קבוע לפרויקטי קוד פתוח בעולם, דוגמת אנשים כמו חוקר אבטחת המידע המפורסם דן קמינסקי או פרופ' דניאל ג'יי ברנשטיין, ולמרות זאת לא ידועות חולשות שהתגלו במערכות אחרות שהם פיתחו שהתגלו על ידי "למידת שגיאות קוד אופייניות להם".

38. אוסיף ואומר, שלנוכח תוצאות הבדיקה המפורטות בפרק VI, יש חשיבות מאוד גדולה בחשיפת קוד המקור של המחשבון כדי לאפשר וידוא כי המחשבון עצמו איננו שולח את המידע לשרתים חיצוניים לשרתי המוסד לביטוח לאומי ו/או מכיל אפשרויות מעקב אחרי המשתמש. וידוא שכזה אפשרי רק עם גישה לקוד המקור עצמו.

39. לסיכום, אין בספרות המדעית ו/או המקצועית תמיכה בטענה שפתיחת קוד כללי יש בה כדי לפגוע באבטחת המידע של הארגון. להפך, בהקשרים בהם יש צורך באמון הציבור שהמידע לא מעובד בדרכים לא רצויות, והגנה על פרטיות למשתמשים, יש דווקא מקום לפרסם את הקוד המשמש את הארגון.

פרק V – כיצד אמור לעבוד המחשבון של המוסד לביטוח לאומי נשוא הבקשה

40. מכיוון שהמחשבון נשוא הדיון הורד מאתר המוסד לביטוח לאומי, אינני יכול לקבוע האם גם הוא עבד בצורה דומה ליתר המחשבונים הנמצאים כרגע באתר המוסד לביטוח לאומי.
41. עם זאת, יש לציין כי לפי אתר המחשבונים שנמצא באתר המוסד לביטוח לאומי, כל המחשבונים שבדקתי ובחנתי אינם מתחברים למערכות הפנימיות של המוסד לביטוח לאומי.
42. המשתמש במחשבון עונה על סדרה של שאלות שבסופן מתקבלת תשובה מהמחשבון (לדוגמא, קיומה של זכאות לדמי אבטלה או גובה דמי האבטלה).
43. מקריאת איפיון המחשבון נשוא הדיון, נראה כי הוא פעל באופן דומה – המשתמש סיפק את כל המידע למחשבון, והמחשבון השתמש בהם ובנוסחאות המוטמעות בו, כדי לקבוע את התשובות.
44. כלומר, אמנם קטעי הקוד הקשורים למחשבון מאוחסנים באתר המוסד לביטוח לאומי, אבל הם אינם מבצעים שום תקשורת עם מערכות פנימיות של המוסד. יתר על כן, אילו אפשר היה "להוריד" את אותם מחשבונים למחשב המשתמש, לא הייתה נוצרת שום בעיית אבטחת מידע מטעם אותם מחשבונים (שאילו היו נדרשים לקבצי "עדכון", דוגמת קובץ המכיל נתוני מדד המחירים לצרכן, היו יכולים לפנות לחלק באתר המוסד לביטוח לאומי שאיננו דורש שום הזדהות ומכיל קובץ סטטי לחלוטין עם המידע הנדרש).
45. הסיבה היחידה שהמחשבונים אינם בעצם ניתנים להורדה (או כתוכנית או כאפליקציה לטלפון חכם) היא בעיה בכתיבת תוכנית שתרוץ על כל סביבות העבודה הקיימות בעולם. לפיכך נהוג לשים מחשבונים ככאלה כחלק מאתרי אינטרנט, אליהם ניגש המשתמש תוך שימוש בדפדפן, דוגמת כרום או Edge (היורש של Microsoft Explorer).
46. במקרים אלה, המחשבון מקבל מידע מן המשתמש, ומפעיל עליו את החישוב שהוגדר בו. מכיוון שהוא איננו "מושך" מידע מתוך מאגרי המידע של הביטוח הלאומי, ברמת העקרון, בהנחה שתהליך התכן (design) של מערכות המוסד ביטוח הלאומי הוא נכון ובטוח, אותו מחשבון אמור לשבת על שרת שלא מכיל מידע פרטי (לדוגמא, תחת שרת אינטרנט אחר) מטעמי אבטחת מידע.
47. יתר על כן, המחשבון לא אמור לשמור את המידע המגיע מן המשתמש, ככה שגם מידע שסופק למחשבון על ידי משתמשים אחרים במחשבון, לא אמור להשמר ולהיות זמין לשרת (מלבד אולי ברגעי החישוב).
48. מכיוון שכך, המחשבון ניתן (ואף רצוי מבחינת אבטחת מידע) שיהיה ממומש כולו בסביבת הדפדפן – הדבר הן יצמצם את סיכוני אבטחת מידע לשרת ויקטין את הסיכוי לגניבת מידע.
49. בנוסף לאמור לעיל, שמירת מידע המגיע מהמשתמש, באופן בלתי קשור למטרה לצרכי השמירה, דורשת יידוע המשתמש. נכון לבדיקתי ברגע כתיבת חוות הדעת, דף המחשבונים באתר המוסד לביטוח לאומי מבטיח כי המידע איננו נשמר (צילום מסך של דף המחשבונים מצורף כנספח לחוות דעתי).
50. יוצא דופן מסוים עשוי להיות שמירת מידע שהוזן כחלק מקבצי המעקב, הלוגים, המשמשים לרוב לצרכי אבטחת מידע.
51. מכיוון שהמוסד לביטוח לאומי מצהיר כי המידע איננו נשמר, הנחת העבודה של המשך חוות דעת זו היא שגם שמירה מטעמי אבטחת מידע איננה מתרחשת.
52. עם זאת, גם אם המידע נשמר בקבצי המעקב, הדבר יכול להתרחש באחד משני אופנים עיקריים – הראשון הוא מטעם הקוד שפותח (כלומר, המחשבון בעצמו שומר מידע בקבצי המעקב) או רכיב אבטחת מידע ארגוני (לרוב רכיב בשם Web Application Firewall, או בקיצור WAF). במקרה שמשתמשים במוצר WAF, הרי שפעולת השמירה בקובץ המעקב איננה נגרמת על ידי הקוד, ולכן, איננה חושפת מידע על מנגנוני האבטחה (וגם, ניתן להניח שרכיב אבטחת המידע, מוגן באופן יחסי).
53. כאשר אנו דנים בשימוש בלוגים מתוך קוד המחשבון עצמו, יש לציין כי מרבית המפתחים אינם ממציאים את גלגל קבצי המעקב מחדש, ומשתמשים במספר ספריות נפוצות. מכיוון שמספר

הספריות בשימוש הוא מצומצם, הרי שתוקף יכול מראש להניח כי המחשבון משתמש באחת ממספר מצומצם של אפשרויות, כלומר, אין יתרון בהסתרת הספריה הרלוונטית.

54. כלומר, אילו פותח המחשבון לפי שיטות אבטחת המידע הנפוצות ביותר (הידועות כ-best practices), אין שום מניעה אבטחתית לחשוף את המחשבון.

פרק VI – תגובות ספיציפיות לטענות העומדות בנספח 1 לכתב התשובה המתוקן

55. סעיפים 14 עד 16 בכתב התשובה מנסים לקבע את הטענה שקוד איננו מידע. מבלי להיות מומחה במשפטים ובהגדרות החוקיות של מהו מידע, אינני סבור כי טענה זו נכונה, ובמיוחד למחשבון עזר אשר נמצא באתר ממשלתי.
56. כדי לסתור את הטענה, אתייחס למקרה היפותטי בו עולה הטענה כי טופס מסוים של גוף ממשלתי מנוסח בצורה מבלבלת, המונעת מאדם מסוים לממש זכות מסוימת. במקרה דנן, ברור כי לבית המשפט (ובוודאי גם לעותרים) צריך להנתן עותק הטופס לצורך בחינה האם יש בעיה בטופס. דוגמא בולטת לכך היא טופס ההצבעה בבחירות לנשיאות ארה"ב בשנת 2000 שהגיעו עד בית המשפט העליון של ארה"ב וקבעו את תוצאות אותן בחירות.
57. לפיכך, אם מחשבון מיצוי זכויות מסוים, עשוי לגרום בטעות למשתמש בו לחשוב שלא עומדת לו זכות מסוימת (לדוגמא, בעת חישוב חבות מס, עקב טעות בקוד, משתמש באתר עשוי לחשוב שאיננו זכאי להחזר, למרות שהוא זכאי לו), הרי שאותו משתמש עשוי להפגע כספית. והדרך החוקית היחידה בה יכול אותו משתמש לבדוק האם הוא נפגע, היא בחשיפת הקוד בפניו.
58. יתר על כן, לתפישתי, מידע הוא כל דבר אשר יכול לתמוך בתהליך קבלת החלטות. לפיכך, אם תהליך קבלת ההחלטות נסמך על פלט של תוכנה מסוימת, הרי שיש לאפשר למי שמעוניין בהבנת תהליך קבלת ההחלטות גישה לאותו פלט.
59. במיוחד הדבר דרוש כאשר הבנה מלאה של איכות מערכת הקוד, דורשת מספר גדול של דוגמאות (לצרכי בדיקת נכונות המערכת).
60. סעיפים 17 ו-18 בחוות הדעת מציינים את עמדת המוסד לביטוח לאומי ואת העובדה שהמוסד לביטוח לאומי בתהליכי הכרה כתשתית מידע קריטית.
61. מבלי להכנס לבסיס החוקי של ההכרה כתשתית מידע קריטית (מכיוון שהיא נסמכת על החלטות ממשלה, דוגמת ב/84 והחלטות ממשלה 2443, 2444 3270, ו-3611), יש לציין כי כל עוד לא הוכרה תשתית מסוימת כתשתית מידע קריטית – הרי שההגבלות, אם קיימות (וכאמור, לדעתי כמומחה, אין הגבלה במקרה דנן, בחשיפת הקוד, גם בהקשרי אבטחת מידע) אינן בתוקף, ולכן אין למוסד לביטוח לאומי עילה להתלות בסוגיות בטחון המדינה בהקשר תביעה זו.
62. סעיף 19 של חוות הדעת מעלה טענה עובדתית – חשיפת קוד מקור טומנת בחובה פגיעה באבטחת הסייבר ובבטחון המדינה. כאמור לעיל, טענה זו איננה נכונה.
63. סעיף 20 של חוות הדעת מציין עובדה שאינני יכול לבדוק. עם זאת, אציין שאין אף מערכת הגנה המציעה הגנה של 100%. אם נניח כי מערכות ההגנה של המוסד לביטוח לאומי מצליחות להתמודד בהצלחה עם 99.99% מהתקיפות המשמעותיות, הרי שלפי סעיף זה, המוסד לביטוח לאומי אמור להנזק מכ-100 תקיפות מוצלחות כל חודש. מכיוון שהנתון הזה איננו סביר, אינני סבור כי אכן המוסד לביטוח לאומי עומד בפני מיליון תקיפות משמעותיות בחודש.
64. אציין בנוגע לסעיף הקודם, כי ברור שההגדרה של מהי תקיפה משמעותית איננה מדויקת. ללא פילוח מדויק לא ניתן לדעת כמה מן ההתקפות הללו הן מתקפות מסוג דיוג (פישינג) כנגד עובדי המוסד ביטוח הלאומי (שלא יושפעו מפרסום הקוד), כמה מתוכן הן כנגד מערכות המייל של הארגון ועוד. עם זאת, יש לציין כי דו"ח סיכום השנה לשנת 2023 של מערך הסייבר הלאומי מציין כ-3380 ארועים משמעותיים במדינת ישראל בשנת 2023. יתר על כן, הן 4 החולשות העיקריות שנוצלו בשנת 2023 לצרכי "אירועים משמעותיים" אלה והן וקטורי התקיפה הנפוצים המוזכרים בדו"ח, אינם מושפעים מחשיפת קוד מקור של מחשבון.
65. למיטב הבנתי, המחשבון המבוקש, אינו מסתמך על נתונים פנימיים של המוסד לביטוח לאומי. על המשתמש להכניס לתוכו את כל פרטי המידע הנדרשים. לפיכך, הקוד בשימוש לא אמור לגשת למאגרי המידע של המוסד לביטוח לאומי, ולפיכך, הוא לא אמור להכיל אף אחד מן הפרטים שבהמשך חוות הדעת בנספח מוזכרים כפוגעים באבטחת המידע.

66. סעיף 23.1 של חוות הדעת דן בחשיפת דרכי גישה לבסיסי ומאגרי מידע – אשר במחשבון דנן, לא אמורים להיות קיימים.
67. סעיף 23.1 גם טוען שהמחשבון חושף שיטות אבטחת מידע – ראשית יש לציין כי הנחת העבודה בקרב מומחי אבטחת מידע היא שלתוקף תמיד יש ידיעה מה השיטות והמנגנונים בשימוש. עקרון זה, הידוע בשם עקרון קרכהוף, הוא עקרון בסיסי באבטחת מידע. במיוחד הדבר נכון בגוף ציבורי שאת רכש מוצרי אבטחת המידע שלו הוא מחויב לבצע במכרז, או בגוף אשר משתמש בהליכי פיתוח בטוחים, דוגמת אלה המוצגים בסדרת תקני אבטחת המידע ISO 27000.
68. אוסיף ואציין כי אם כל אבטחת המידע והסייבר של מערכות המוסד לביטוח לאומי עומדות ותלויות על סודיות קוד של מחשבון אחד (שלא אמור להתחבר למערכות פנימיות של המוסד לביטוח לאומי), הרי שיש לבצע באופן תדיר בדיקות אבטחת מידע למערכות שבהן פותח הקוד (כדי להמנע מפריצה אליהן על ידי גורמים עוינים), לבצע בדיקת רקע בטחונית מלאה למפתחי הקוד ועוד. הדבר נכון במיוחד לנוכח ההכרה המתקרבת של המוסד לביטוח לאומי כתשתית מידע קריטית.
69. סעיף 23.2 של חוות הדעת מעלה טענה מעניינת חשיפת קוד המקור של תוכנה מגדילה את הפגיעות. כאמור בפרק III של חוות דעתי, טענה זו לא הוכחה כנכונה. יתר על כן, אציין כי תוקפים אשר יכולים לייצר איומי סייבר משמעותיים, לדוגמא, קבוצות תקיפה הפועלות בשירות מדינות עוינות דוגמת אירן, יכולות להגיע לקוד המקור. כלומר, מלכתחילה צריכה הנחת העבודה של כל מומחה אבטחת מידע המתעסק עם תשתיות מידע קריטיות להיות שקוד המקור חשוף בפני הרוצים להרע לו. לפיכך חשיפת הקוד איננה משנה את ניהול הסיכונים כהוא זה.
70. יתר על כן, במקרה דנן, מדובר בקטע קוד שאמור להיות מנותק ממערכות המוסד לביטוח לאומי, לא מתחבר אל שרתיו לצורך גישה אל מידע, אלא מחשבון שלוקח את הנתונים שהקיש המשתמש ומחשב על פי נוסחא קבועה מראש את התוצאה. כאמור בפרק IV של חוות דעתי, אין בקוד כדי להכיל דברים סודיים או רגישים.
71. מכיוון שהנוסחא עצמה איננה סודית (היא תוצר של דו"ח ציבורי), ומכיוון שאף אחד מהנתונים הנדרשים לה איננו אמור להשלף ממערכות המוסד לביטוח לאומי, הרי שהקוד בו אנו דנים לא אמור להכיל אף מנגנון התחברות לשרתי המוסד לביטוח לאומי, איננו מכיל מידע סודי בדרך חישוב הנוסחא, ויש לומר, שלהפך – אם הוא מכיל רכיבים שכאלה, הרי שאיפיון המערכת שגוי מיסודו.
72. סעיף 23.3 של חוות הדעת טוען כי חשיפת הקוד תאפשר זיהוי פגיעויות בקוד (ומונה רשימת מעשין ובעשין שיכולה לקרות). עם זאת, בהנחה שהקוד פותח בהתאם למדריכי הפיתוח הבטוח (ובמיוחד בהקשר זה, נבדק הקלט שמכניס אליו המשתמש ככזה שאינו מכיל קוד זדוני), ובהנחה שהוא יושב בסביבה של אתר המוסד לביטוח לאומי שאיננה מתקשרת עם מאגרי המידע של המוסד לביטוח לאומי, הרי שהסכנה היחידה שיכולה להיות היא קלט זדוני של המשתמש. ישנן מספר דרכים לצמצם את הסכנה שקוד כזה מהווה לשרתי המוסד לביטוח לאומי, לדוגמא השימוש בכלי אבטחת מידע דוגמת WAF-ים שהוזכרו קודם לכן. כמובן, שהמערכת עצמה לא תפגע אם יחשף השימוש במנגנון WAF.
73. עובדה המכבידה על קבלת טענות חוות הדעת בכתב התשובה המתוקן היא העובדה שהקוד של המחשבון כבר איננו פעיל באתר המוסד לביטוח לאומי. כלומר, גם אם תוקף זדוני יזהה בקוד חולשה, הרי שהקוד איננו פעיל, ולכן כל חור אבטחה שבו איננו יכול להשפיע על המערכת באופן ישיר.
74. סעיף 23.4 טוען כי חשיפת קוד המחשבון תאפשר לתוקף לגלות את ממשקי המוסד לביטוח הלאומי עם גופי ממשל אחרים (ובכך להגדיל את סיכון הסייבר שלהם). עם זאת, המחשבון האמור מקבל את כל המידע שלו מהמשתמש (ואם הוא נעזר במידע משרתי הביטוח הלאומי, זהו מידע פומבי, דוגמת מדד המחירים לצרכן), ולכן טענה זו איננה רלוונטית למחשבון נשוא הבקשה.
75. סעיף 23.5 מציין כי חשיפת הקוד תאפשר פיתוחם של מתקפות יום אפס (zero-day) . אלו מתקפות מאוד עוצמתיות, מכיוון שהן מתקפות ש"טרם נתקלנו בהן", ולכן הרבה מרכיבי אבטחת המידע אינם יודעים להתמודד עמן באופן מפורש.
76. עם זאת, המחשבון נשוא הדיון הוא לכאורה מימוש של טופס פשוט. חשיפת קוד המקור שלו לא אמורה לחשוף פגיעויות חדשות בשום מערכת תוכנה (כמו שרתי האינטרנט שעליהם פועל אתר המוסד לביטוח לאומי).
77. לסיכום שתי הנקודות הנ"ל בחוות דעתי, היה מוטב לו סעיף 23.5 לא היה בא לעולם, והטענות שבו לא היו מועלות.

78. סעיף 23.6 של חוות הדעת מציין כי חשיפת קטע הקוד עשוי לחשוף את המבנה הפנימי של מאגרי המידע של המוסד לביטוח לאומי. עם זאת, המחשבון הרלוונטי איננו משתמש בשרתי המוסד לביטוח לאומי, ולכן לא ברור על מה מסתמכת טענה זו.
79. לסיכום הטענות בנוגע לסעיף 23 של חוות הדעת בכתב התשובה, כמי שמלמד אבטחת מידע מאז 2004, כמי שמשמש כנציג ישראל לועדת התקינה של ארגון התקינה בנושאי אבטחת מידע מ-2017, וכמי שמעורב במחקר פעיל בתחומי אבטחת מידע מאז 1998, העמדות המוצגות בסעיף 23, אינן רלוונטיות למחשבון המדובר, וחלקן גם אינו עולה בקנה אחד עם הידע המדעי והמקצועי בתחום.
80. סעיף 24 של חוות הדעת בכתב התשובה מציינת את כל הבעיות העלולות להווצר לפרטיותם של משתמשים לנוכח בעיות הסייבר המתוארות בסעיף 23 של חוות הדעת. כאמור, הטענות בסעיף 23 אינן רלוונטיות למחשבון נשוא הדיון, ולכן כל המסקנות על הפגיעות האפשרויות המתוארות בסעיף 24 הן רשימת מכולות של איומים אפשריים, ותו לא.
81. הסעיף היחיד הרלוונטי לקוד המחשבון המפורש הוא סעיף 24.2 המציין כי קוד המקור של המחשבון עשוי להכיל "מידע רגיש כגון מפתחות הצפנה, סיסמאות, פרטי גישה למערכת". אמנם, קוד מקור עשוי להכיל פרטים אלה, אבל בהקשר של המחשבון דנן, כאמור, לא אמורות להיות בו סיסמאות או מפתחות הצפנה או פרטי גישה למערכת, מכיוון שהוא אמור לרוץ בצורה מנותקת מהמידע של המוסד לביטוח לאומי.
82. יתר על כן, שמירת מפתחות הצפנה ו/או סיסמאות ו/או פרטי גישה למערכת באופן שמופיע בקוד באופן קבוע היא מתודת פיתוח נוראית, הנחשבת מסוכנת, ואיננה עולה בקנה אחד עם אף מדריך לפיתוח קוד בטוח.
83. כלומר, סעיף 24.2 דן בפגיעה שלא אמורה להתקיים, כי המחשבון נשוא הדיון לא אמור להכיל פרטים שכאלה. שנית, גם אילו היה צורך בפרטים אלה במחשבון (לדוגמא, לצורך גישה פנימית למידע של שרתי המוסד לביטוח לאומי), קביעתם בקוד בצורה מפורשת היא שגיאת פיתוח מהמעלה הראשונה, ואיננה אמורה להתרחש לפי אף מתודת פיתוח תוכנה. יתר על כן, נניח כי המפתח של המחשבון החליט לעשות טעות כפולה ומכופלת, ולהכניס פרטי חיבור (שאינם דרושים) באופן מפורש לקוד (בצורה שחורגת מה-best practices), הרי שמעבר פשוט על הקוד וסילוק אותם רכיבים (בדומה להשחרה של פרטים רגישים) בטרם חשיפת הקוד לציבור הינו פעולה פשוטה ומהירה. כלומר, בהנחה שהקוד פותח ותועד כהלכה, כל מתכנת יכול לבצע את הפעולה הזו במספר דקות מועט.
84. סעיף 24.2 גם חוזר על הטענה כי חשיפת הקוד תגלה מהם מנגנוני ההגנה בהם משתמש המוסד לביטוח לאומי. כאמור בחוות דעתי זו, טענה זו מתנגשת התנגשות חזיתית עם ה-best practices הנהוגים בתחום אבטחת המידע, ואשר עומדים בסתירה לעקרון קרכהוף.
85. סעיף 25 חוזר ברובו על הטענות המופיעות בסעיפים 23 ו-24, שכאמור, אינן מדויקות.
86. סעיף 25 אף מוסיף שתי טענות – הראשונה בסעיף 25.6 הקובע חובת אישור של ועדה מייעצת. לעניות דעתי, אין מניעת אבטחת מידע בנוגע לקוד הרלוונטי (כפי שמתואר בעיקרי חוות הדעת הזו). אוסיף ואומר שעל פניו נראה כי המחשבון המסוים שהוא נשוא הדיון לא מכיל נושאי קניין רוחני מהותי, ולכן בסיס הטענה איננו נהיר לי.
87. סעיף 25.7 דן בנהלי עבודה פנימיים של גופי ממשלה וציבור (וטוען שהכלל הציבורי איננו תקף). אין לי להוסיף או להחסיר בנוגע לטענה.
88. סעיף 26 מעלה טענה לפגיעה באמון הציבור עקב פרסום קוד מקור. מחקרים לאורך שנים מראים כי טענה זו איננה נכונה. כדוגמא נגדית אציין כי בתחום בו אמון הציבור הוא אחד מהגורמים המהותיים ביותר לתהליך כולו – בחירות אלקטרוניות – מכיל המדריך המקיף ביותר בתחום (ה- Voluntary Voting System Guidelines (VVSG) 2.0), בפירוש המלצה לוידוא חיצוני של קוד המקור של המערכת (סעיף 13.2), בדיקה שמדובר בשיטות תכנות מוכרות ומתאימות (דרישה 2.1-C המציינת במפורש שמדובר בשיטות תוכנות שפורסמו וידועות לציבור), מסביר כיצד לוודא מקוריות של קוד פתוח (דרישה 3.1.1), ומכאן למדים אנו ששימוש בקוד מקור פתוח מותר למערכות כאלה, בדיקת הקוד על ידי גורם חיצוני לפרויקט (כלומר הקוד נחשף לאחרים, כמו לדוגמא בדרישה 9.1.6) ובמיוחד היתרונות של פרסום הקוד לציבור (כפי שהודגם במאמר של Thomas Haines et al. – "How not to prove your election outcome" שהוצג בכנס אבטחת המידע מהמובילים – Security and Privacy 2020).
89. סעיף 27 של חוות הדעת דן בקניין הרוחני של המוסד לביטוח לאומי. אינני מומחה בתחום (ולמיטב ידיעתי גם חותם חוות הדעת איננו מומחה בקניין רוחני), כך שלמשקל הטענות בו אינני יכול

להתייחס. עם זאת, במדינות רבות נהוג כי קניין רוחני של גופי ציבור, משותף לטובת כלל אזרחי המדינה. יתר על כן, אם יורשה לי לציין כי בנושא המחשבון דנן, לא הובהר בחוות הדעת כי יש קניין רוחני מהותי (לעניות דעתי, תוכנה אשר מבצעת חישוב מתמטי פשוט המבוסס על נוסחא הידועה לציבור, ואשר יושב בתוך אתר אינטרנט, איננה מכילה חדשנות טכנולוגית מספקת כדי להנות מהגנות קניין רוחני).

90. סעיפים 28 ו-29 של חוות הדעת דנים במחשבון דנן ומפרטים את תכולתו.

91. סעיף 31 מעלה טענה כי תוקף שיכול לבחון את הקוד של מחשבון יוכל לחשוף מידע על "ארכיטקטורת המערכת, שיטות עבודה, ונקודות תורפה אפשריות..." כאמור לעיל, מדובר במחשבון שאיננו מתחבר לתוך מערכות המוסד לביטוח לאומי ולא אמור להכיל מידע סודי (שגם אם במקרה הוא כן, ניתן להוציאו בקלות). יתר על כן, בהנחה ששיטות העבודה של מפתחי הקוד הן ה- best practices הנהוגים בתחום, הרי שתוקף יודע מהן שיטות העבודה של מפתחי הקוד.

92. סעיף 32 מפרט את הרכיבים שהמחשבון עשוי להשתמש בהם. מלבד העובדה שהמחשבון דנן לא אמור להכיל אף אחד מהפרטים המוזכרים בסעיף (הוא לא אמור לגשת לטבלאות פנימיות בשרתים פנימיים, מכיוון שהוא איננו מכיל מידע אישי ו/או טוקני הרשאות, כפי שנטען בחוות דעתי זו מספר פעמים), זיהויים והסרתם בקלות אפשרית.

93. סעיף 34 מציין כי יתכן והמחשבון משתמש בספריות מיושנות ו/או לא מאובטחות דיין. כולי תקווה כי מערך המיחשוב של המוסד לביטוח לאומי מוודא כי כל שירותיו משתמשים בספריות מעודכנות, וכי כאשר הוא רוכש שירותי פיתוח תוכנה חיצוניים הוא דואג לדרוש אחריות ושירות כדי לוודא שבעיות כמו זו המתוארת בסעיף 34 לא מתקיימת.

94. סעיף 35 מציין כי הקוד הרלוונטי עשוי לחשוף קיומן של ספריות פנימיות של המוסד לביטוח לאומי. לכותב חוות דעת זו אין גישה לקוד המחשבון כדי לוודא האם קיימות כאלו ספריות. עם זאת, מצופה היה מחוות הדעת של המוסד לביטוח לאומי לא לטעון טענה על "האפשרות הזו" אלא לציין במפורש האם היא ממומשת.

95. אוסיף ואציין שכאמור, המסקנה של סעיף 35, גם אם קוד המחשבון משתמש בספריות פנימיות של המוסד לביטוח לאומי, איננה תואמת לידע המדעי והטכנולוגי המצוי.

96. סעיף 36 מעלה טענה כי חשיפת הקוד תציג בפני התוקפים מפת דרכים לתכנון מתקפות ופריצות. בהנחה כי המוסד לביטוח לאומי נוקט בשיטות פיתוח קוד תקניות (best practices) או דורש שימוש בכאלה במכרזיו, הסיכון הנובע מחשיפת הקוד היא מזערית (אם בכלל קיימת).

97. סעיף 37 מציין כי עקביות בשיטות הפיתוח, פירושן שחשיפת קוד מן העבר יש בה כדי לפגוע בבטחון הנוכחי. בסעיף זה יש בלבול מסוים בין בעיות בשיטות הפיתוח (שהפתרון להן הוא שימוש ב- best practices הקיימים בעת פיתוח הקוד) ובין בעיות בספריות קיימות (שגם הן כאמור, צריכות להיות משודרגות ומוגנות). יתר על כן, פיתוח קוד כך שהוא יהיה תלוי ככל הפחות בגרסא מסוימת של ספריה מסוימת היא מתודת פיתוח תוכנה נפוצה בעולם.

98. סעיף 38 מעלה את החשש של פיתוח תקיפות ייעודיות למערכות המחשב של הביטוח הלאומי. כאמור, המחשבון נשוא הבקשה הוא טופס אליו מעלה המשתמש מידע יחד עם שימוש בנוסחא פומבית. על פניו, לא ברור על מה מסתמכת הקביעה כי "חשיפת קוד המקור מגבירה, באופן משמעותי," את הסיכון. כאמור בפרק III של חוות דעת זו, קוד מקור פתוח איננו נחשב כמגביר את הסיכון של מערכות מחשב למתקפות אלה ואחרות.

99. סעיף 39 מתקשר לסעיף 38, ומתאר את הדרך בה אותן תקיפות ייעודיות יכולות להתפתח, קרי תוך שימוש בטכנולוגיות הנדסה לאחור ואבחנות על הלוגיקה העסקית בבסיס התהליכים. בהנתן היקף הקוד הצפוי של המחשבון, צורת פעולתו (המקבלת את כל המידע מהמשתמש ואיננה שומרת אותו), עמדתי המקצועית היא שסעיף זה אין לו במה להאחז.

100. סעיף 40 של חוות הדעת מעלה חשש לפגיעה בשרשרת האספקה של הקוד שבשימוש. כלומר, זיהוי אותן ספריות אשר בשימוש תוכנות ומחשבונים של המוסד לביטוח לאומי. בבסיס הסעיף עומדת טענה נכונה אך בהקשרים של קוד הנמצא באינטרנט שאפשר לבצע לו בדיקה (כפי שמתואר בפרק הבא), טענה זו מתעלמת מהעובדה שהספריות והכלים שבשימוש המחשבונים הקיימים של המוסד לביטוח לאומי הם ידועים לכל. אי לכך, בעוד הטענה נכונה, היא לא יכולה להתקיים בעולם בו המוסד לביטוח לאומי מפעיל מחשבונים אחרים שזמינים לציבור.

101. סעיף 41 טוען שחשיפת הקוד עומדת בניגוד לנהלי אבטחת המידע הקיימים. מכיוון שאלה אינם זמינים לי, איני יכול לחוות את דעתי על הטענה עצמה. עם זאת, יתכן ונהלי אבטחת המידע

הללו נכתבו בניגוד לידע המדעי והטכנולוגי העומד לרשותינו, וייתכן שמן הראוי לתקף אותם בראי חוות דעת זו.

102. סעיף 42 מסכם את שלל טענות הפרק (סעיפים 41-28).

103. יש לציין כי סעיפים 42-28 כולם נטענים בעלמא ללא התייחסות ספיציפית לקוד המחשבון המפורש. בשום סעיף של חוות הדעת לא מציין כותב הדו"ח כי הוא בחן את הקוד הרלוונטי, ומצא בו את אותם סימנים "מחשידים" כגון התחברות לשרתי המוסד לביטוח הלאומי, טוקני הזדהות (דוגמת שמות משתמש וסיסמאות או מפתחות קריפטוגרפיים), או אפילו שמות של טבלאות של מאגרי המידע הקיימים במוסד לביטוח לאומי.

104. יש לציין כי בשנים האחרונות חלה התקדמות אדירה ביכולתיה של ממשלת ישראל לחשוף מידע לחוקרים – דוגמת חדרי המחקר של משרד הבריאות ושל הלשכה המרכזית לסטטיסטיקה. חדרי מחקר אלה מאפשרים לחוקרים גישה (מפוקחת ומנוטרת) למידע רגיש, המאפשרת לבחון את המידע באופן בטוח ומשמר פרטיות. לדוגמא, בהאקתון שערכנו ב-2021 במרכז חקר סייבר משפט ומדיניות (בשיתוף גופים אחרים), פתח משרד הבריאות חדרי מחקר שלו לחוקרים מרחבי הארץ כחלק מניסיון למצוא מזור מבוסס-נתונים למגיפת הקורונה.

105. אם מידע רפואי רגיש (הכפוף לשלל מגבלות חוקיות ואתיות רחבות הרבה יותר מהמחשבון דנן) או מידע רגיש של הלשכה המרכזית לסטטיסטיקה הופכים לנגישים לציבור, קל וחומר שקטע קוד של מחשבון יכולים להחשף באופן דומה, כדי לקבוע באופן מדויק האם הטענות שהעלתה חוות הדעת המקורית בעלות משקל.

פרק VII – בחינת המחשבונים הנמצאים כרגע באתר המוסד לביטוח לאומי

106. כחלק מהניסיון לכתוב חוות דעת זו, נעזרתי במחשבונים הנמצאים היום באתר המוסד לביטוח לאומי.

107. הבדיקה כללה ניסיון להבין כיצד זורם המידע בין המשתמש והמוסד לביטוח לאומי, לזהות האם יש מידע על מבנה הקוד שניתן להסיק כבר היום מהמחשבונים הזמינים באתר המוסד לביטוח לאומי, ולבדוק כמידת האפשר את הטענות שעלו בחוות הדעת של כתב התשובה.

108. למען הסר ספק, כל הבדיקות נעשו על מחשבי שלי, לא כללו פניה לא מורשה לשרתי הביטוח הלאומי, לא שינו את התעבורה אליו (או לשרתים אחרים), וכללו אך ורק בדיקה של מידע העובר בעת הפעלת המחשבון על ידי משתמש רגיל.

109. כלומר, אף אחת מהפעולות שנעשו בבדיקה זו איננה מוגדרת כפעילות התקפית, ומלבד הפעלת המחשבונים שנבדקו, באופן שמחשבונים אלה אמורים להיות בשימוש, לא נעשתה אף פעולה אחרת.

110. במהלך הבדיקה התגלה כי אתר המחשבונים של המוסד לביטוח לאומי מכיל מנגנוני מעקב של חברת גוגל. ספיציפית, כל פעם שמישהו משתמש באתר המחשבונים של המוסד ביטוח הלאומי, מקבלים שרתי גוגל חיווי כי מחשבון מסוים הופעל.

111. כלומר, חברת גוגל, יכולה לדעת כי מחשב מסוים (כלומר, משתמש מסוים), הפעיל מחשבון דוגמת בדיקת זכאות לקצבת נכות או לדמי אבטלה.

112. למותר לציין כי פירוש הדבר כי חברת גוגל יכולה ללמוד רבות על מצבו הבריאותי של משתמש בעצם זה שפנה לקבל מידע על זכאויות שונות. לדוגמא, שאדם מסוים "נדרש" לקצבת נכות. מעבר למידע רפואי (זכאות למענק לידה ו/או נכות), חלק מהמחשבונים חושפים עוד אירועים משמעותיים בחיי האזרח – החל מבדיקת זכאות לקצבת נפגעי פעולות איבה או סיעוד, וכלה בזכאות לתגמולי מילואים. בימים שבהם גורמים זרים אוספים מידע מי מהישראלים משרת שירות מילואים פעיל, העובדה שהמידע הזה נמסר לחברה בינלאומית כגון גוגל (שעשויה להיות מחויבת לחשוף מידע זה לפי דין זר), היא בעייתית ביותר.

113. החשיפה עצמה מתבצעת עקב הטמעת מנגנון מעקב של חברת גוגל בדף המחשבון. בדף המחשבון יש קריאה מפורשת לשליחת מידע לשרתי גוגל. תיאור מקוצר של מנגנון המעקב מופיע בנספח ב'.

114. כלומר, אתר הביטוח הלאומי באופן פעיל חולק מידע בנוגע למצבו של המשתמש עם שרתי חברת גוגל.

115. במהלך בדיקת קוד המקור של המחשבון, הסתבר לי כי מידע על טפסים עשוי להשלח לשרתים היושבים תחת כתובת האינטרנט report.gbpilot.glassboxdigital.io (הוכחה לטענה ניתן

למצוא בנספח ג'). בדיקה ברשם כתובות האינטרנט (שירות הידוע בכינויו whois), גילה כי כתובת זו היא כתובת פרטית ומוגנת. כלומר, מידע ממחשבונים באתר הביטוח הלאומי נאסף, ונשלח לחברה שזהותה אנונימית.

116. למה דומה הדבר המתואר בסעיף הקודם? לכך שהביטוח הלאומי יקח את כל (או חלק מן) הטפסים, ישים אותה במעטפה עלומה, וישלח אותם לכתובת לא ידועה. ללא יכולת בקרה של הציבור ו/או בכלל יידועו שכך נעשה.

117. אחת הדרכים היחידות לוודא שמקרים כאלה אינם קורים בתוך קוד המחשבון עצמו (ולא רק בקוד האתר שבו נמצא המחשבון), ובוודאי הדרך המהירה ביותר, הנוחה ביותר, וגם זאת שלא חושפת את שרתי המוסד לביטוח לאומי למתקפות סייבר נוספות, היא לחשוף את קוד המחשבון עצמו.

פרק VIII – סיכום:

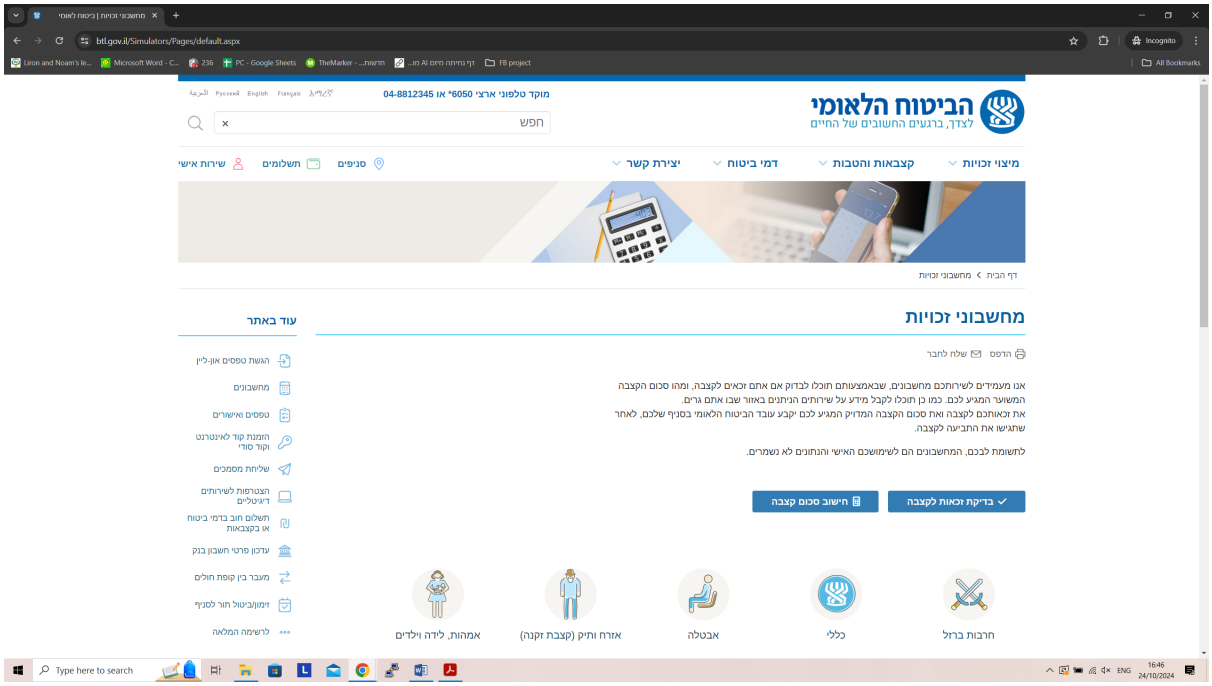
118. כפי שהראתה חוות דעתי זו, אין בעית אבטחת מידע בחשיפת קוד מקור של מחשבון, בין אם הוא כרגע בפעולה או לא בפעולה.

119. כתוצאה מכך, אין חשיפת קוד המקור יכולה לגרום לפגיעה בפרטיות משתמשי האתר.

120. על אחת כמה וכמה, לנוכח בעיות מסוימות באתר המוסד לביטוח לאומי, יש חשיבות אבטחתית וחשיבות לפרטיות, לבחינה מעמיקה של קוד המקור של המחשבון דנן (ושל יתר המחשבונים) כדי לוודא שהוא לא שולח מידע אל מחוץ לשרתי המוסד לביטוח לאומי.

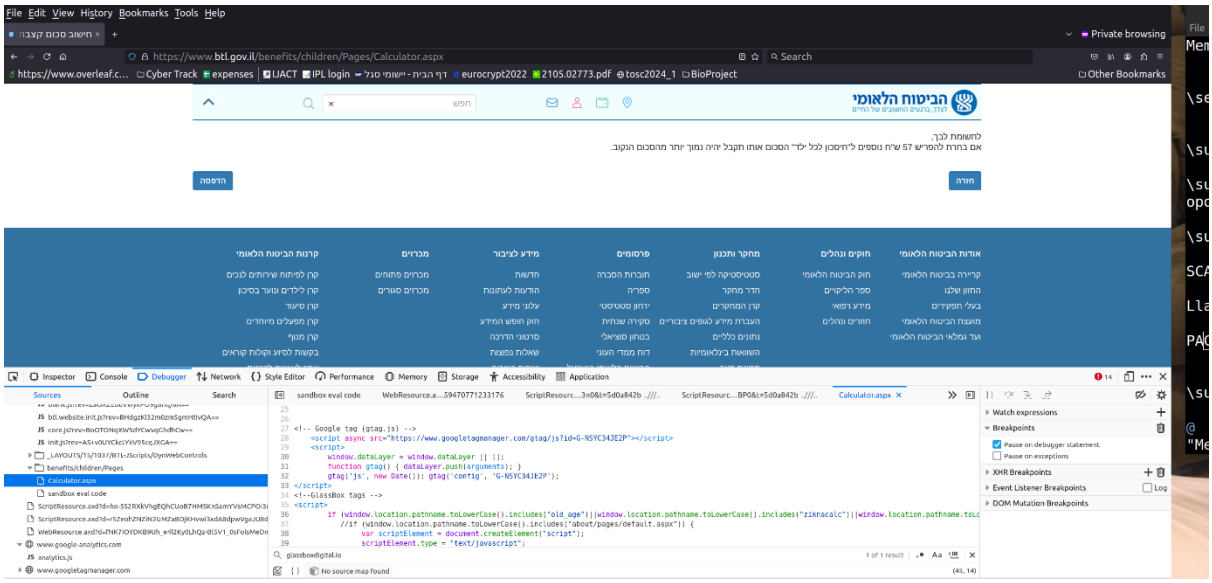
נספח א':

אתר מחשבוני הזכויות של המוסד לביטוח לאומי – וההצהרה כי איננו שומר מידע.



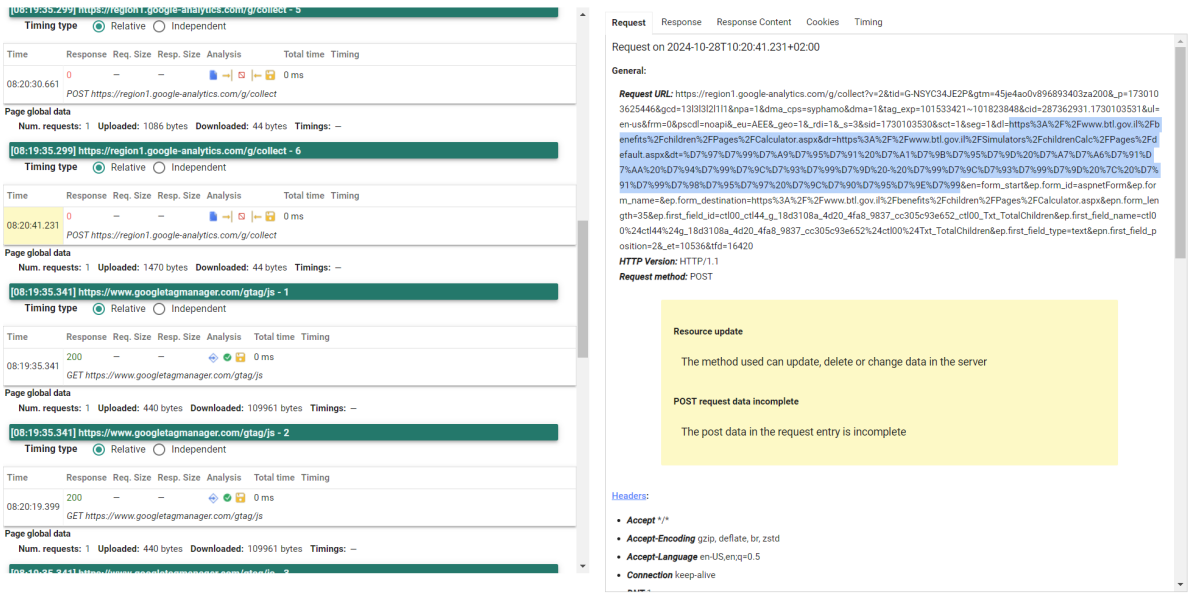
נספח ב':

קיומו של סקריפט המעקב של חברת גוגל באתר המחשבונים של הביטוח הלאומי.



ניתן לראות במפורש את השורה <scrypt async src="...."> אשר מכילה הוראה לדפדפן האינטרנט של המשתמש לקרוא לקוד המעקב של חברת גוגל.

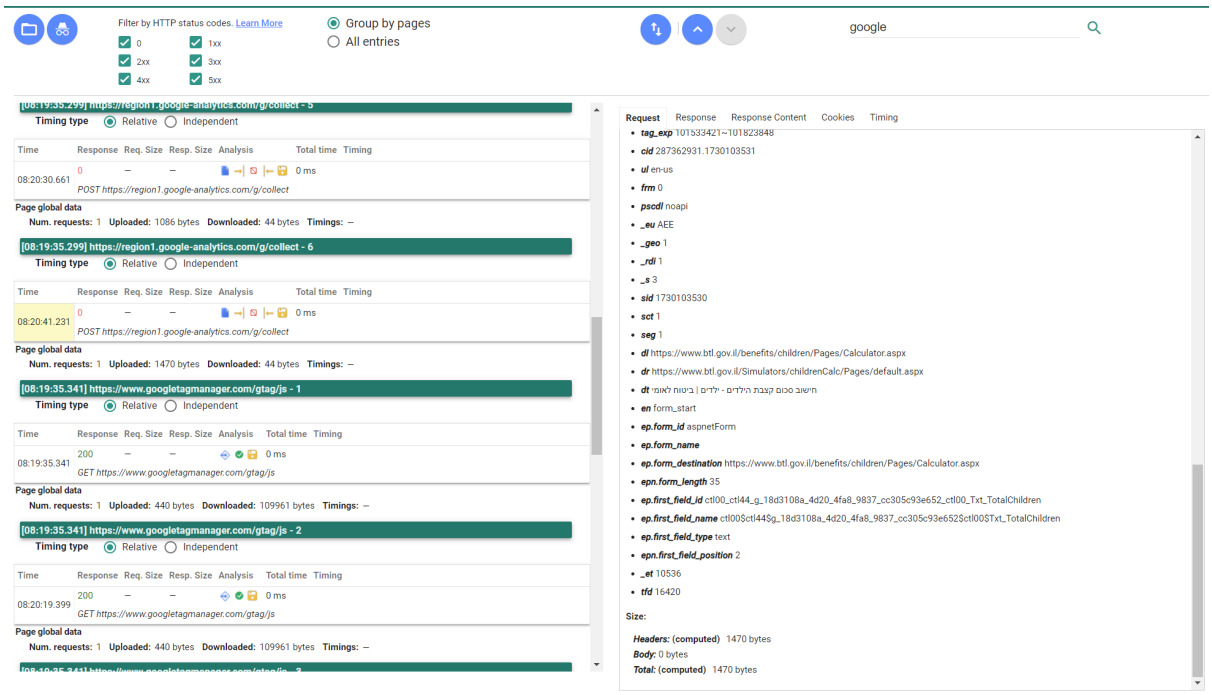
מכיוון שחברת גוגל מפעילה מספר שרתי למעקב אחרי מידע, בדקתי גם את המידע הנשלח לשרתי גוגל.
לדוגמא, בעת הגלישה למחשבון זכאות לקצבאות ילדים, נשלח המידע הבא לשרתי חברת גוגל:



אמנם המידע שנשלח תחת השדה – Request URL נראה מורכב למדי, אבל בעצם זהו אחד ממנגנוני המעקב של גוגל. בעצם דפדפן המשתמש מנסה לגשת לכתובת הרשומה בתוך השדה Request URL. הדבר דומה לגישה לדפים שונים הנמצאים בשרת מסוים (לדוגמא, כניסה לכתובת https://supreme.court.gov.il/Pages/HomePage.aspx תוביל לאתר בית המשפט העליון, בעוד כניסה לכתובת https://supreme.court.gov.il/Pages/Overview.aspx תוביל לדף "על אודות" באתר בית המשפט העליון).

במקרה זה, חברת גוגל מתאימה לכל אתר לינק אישי. בעת גישה לאתר גוגל, לדף שמכיל את השם של אתר הביטוח הלאומי, מחשבי גוגל רושמים שמישהו ניגש לדף שנקרא בשם "חישוב סכום קצבת הילדים – ילדים | ביטוח לאומי", ורושם שהייתה גישה ממחשב מסוים אל הדף תחת השם הזה.

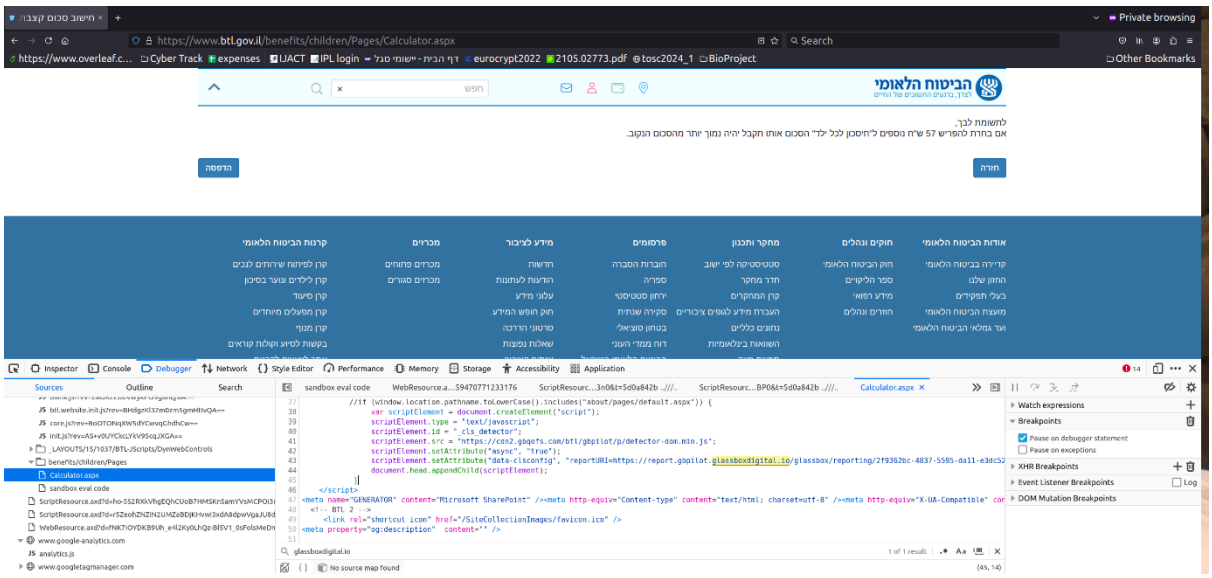
כדי להראות כי זהו שם הדף הרשום, ניתן לקחת את החלק המודגש בכחול, ולבצע קריאה של כתובת ה-URL תוך שימוש בכלים סטנדרטיים. לדוגמא, כלי קריאת נתוני התקשורת של גוגל מאפשר לקרוא את המידע באופן מיידי:



קל לראות כי הבקשה לשרתי גוגל מגיעה יחד עם המידע שהמשתמש ניגש לדף המחשבונים לקצבת ילדים באתר הביטוח לאומי (הן בכתובת הגישה המצוינת והן בטקסט המצורף). תופעה זו כמובן קיימת בכל המחשבונים שבדקתי באתר המוסד לביטוח לאומי.

יש לציין כי חברת גוגל יכולה בקלות לזהות את המשתמש על סמך נתוני תקשורת (זיהוי כתובת האינטרנט ממנה ניגשים לשרתי גוגל), מידע ניהולי דוגמת קבצי עוגיות ששמורים אצל המשתמש (כולל עקב קיומם באתרים אחרים שאליהם גולש המשתמש), ואף שימוש בטכניקות fingerprint סטנדרטיות לחלוטין שיכולות לזהות פרטים על המשתמש (לדוגמא, סוג הדפדפן ומערכת ההפעלה שבה הוא משתמש).

נספח ג':



ניתן לראות כי באתר המחשבון של הביטוח הלאומי, יש שדה של reporting השולח מידע לכתובת האינטרנט report.gbpilot.glassboxdigital.io.