הקמת מרכז לתמיכת באירועי אבטחת סייבר אצל אזרחים

תוכנית עבודה

פברואר 2016

תוכן עניינים

1. מבוא
2. תפישת העבודה להקמת המרכז
3. אתר המידע לציבור
4. מערכות המידע הנדרשות לפעולת המרכז
5. כוח אדם
6. תקציב נדרש

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי
ISOC-IL

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

1. מבוא

א. המונח "סייבר" מתאר עולם תקשורת מחשבים בו כל המחשבים מחוברים ומקושרים האחד עם השני דרך רשת האינטרנט. את המונח "מחשב" יש לפרש באופן רחב, והוא כולל מחשבים ארגוניים, מחשבים אישיים, אמצעי תקשורת ניידים כגון טלפונים חכמים, אמצעי מדיה כגון טאבלט או טלויזיה חכמה, סנסורים מקושרים (כגון שעונים חכמים) וכל מה שנחשב כ-internet of things.

ב. קישוריות זו טומנת בחובה יתרונות עצומים לחברה ולכלכלה, ומאפשרת פיתוח יישומים מסוגים שונים לשימושם היום-יומי של אזרחים ועסקים. היקף השימוש ביישומי מחשב מקושרים ומידת התלות של האוכלוסיה בהם הולך וגובר מיום ליום.

ג. שימוש נרחב זה ביישומי מחשבים על ידי מדינות, ממשלות, עסקים ואזרחים הביא לצמיחתו של ענף לוחמה, טרור ופשיעה חדש המנצל את הקישוריות האינטרנטית בין שלל המערכות ומגוון המשתמשים בהם להשגת יעדים פוליטיים, מדינתיים, צבאיים, כלכליים ואישיים של התוקף. מחשבים הפכו להיות יעדים לפעילות תקיפה ממוחשבות המנסות לרכוש לעצמן גישה לאותם מחשבים, ואפשור מתן הוראות ביצוע פעולות שונות המשרתות את האינטרסים של התוקף כגון השבתת פעילות המחשב, גניבת מידע ממנו, שימוש לא מורשה בו וכד'.

ד. היעדים לאותן פעולות תקיפה ממוחשבות הן בדרך כלל ישויות כגון ממשלות, גופים עסקיים או גופים שונים ללא מטרות רווח, אך הם יכולים להיות גם אנשים יחידים. לעיתים התוקף מעוניין במידע של אותו אדם (כגון השגת פרטי כרטיס האשראי שלו), ולעיתים השגת גישה למחשבו של אותו אדם משרתת תכלית אחרת במהלך תקיפה של ישות שאינה בשר ודם.

ה. התחום שעוסק בהתגוננות בפני אותם איומי סייבר מוכר בשם "הגנת סייבר", והוא מהווה הרחבה של תחום אבטחת המידע, אשר עסק בעיקרו במחשבים שרמת הקישוריות שלהם הייתה נמוכה ומוגדרת היטב. היקף הקישוריות ומורכבותה הוא שיוצר אתגר חדש המחייב התמודדות שונה מתפישות אבטחת המידע הקלאסיות שהיו קיימות עד תחילת המאה ה-21.

ו. מדינת ישראל משקיעה בשנים האחרונות משאבים רבים בגיבושה של תפישה חדשנית להגנת סייבר מדינתית, בהובלתו של מטה הסייבר הלאומי אשר הוקם בהחלטת ממשלה בשנת 2011. כתוצאה מתהליך הניתוח וגיבוש המדיניות הלאומית, קיבלה לאחרונה הממשלה את המלצת מטה הסייבר והחליטה על הקמת רשות לאומית להגנת סייבר, אשר מתחילה פעילותה בימים אלה. במסגרת הרשות הלאומית להגנת סייבר, מוקם מרכז סיוע להתמודדות עם אירועי סייבר (CERT).

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי
ISOC-IL

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

ז. תקיפת סייבר כנגד אזרח, או עסק קטן, פוגעת בדרך כלל באזרח או בעסק הקטן, אך כשלעצמה אינה יכולה לפגוע בחברה הישראלית. תקיפה שכזו יכולה אמנם לשמש פלטפורמה לתקיפה של גופים גדולים (למשל אם אותו אדם הוא עובד של גוף שהוא יעד לתקיפה), אך בעיקרה היא יכולה לפגוע משמעותית באיכות חייו הוירטואליים, וגם הפיזיים, של אותו אדם. גניבת זהות ומידע אישי, השמדת מידע או לקיחתו של המידע כבן-ערובה, שינוי מידע או שימוש בו לשם השגת נכסים חומריים של אותו אדם הינם איומים הולכים וגוברים על האזרח בעולם המודרני.

ח. בדיונים שהתקיימו בועדת ההיגוי לתשתיות של איגוד האינטרנט הישראלי (להלן – **האיגוד**) בשנים 2014-2015, הוחלט לקדם הקמה של מרכז תמיכת הגנת סייבר לאזרחים ולעסקים קטנים. הבסיס להחלטה זו היא החשיבה כי עיקרה של הפעילות המדינתית מופנה להגנת סייבר בגופים גדולים כגון משרדי ממשלה, רשויות סטטוטוריות, חברות ממשלתיות, גופים המנהלים תשתיות קריטיות ועסקים גדולים מתוך ראיה כי פגיעה בהם עשויה לגרום נזק משמעותי לחברה הישראלית, אך טיפול מותאם לסיכונים לאזרח או לעסק הקטן אינו במרכז העשייה המדינתית.

ט. האיגוד משער שאזרחים ועסקים קטנים ידרשו יותר ויותר להדרכה והכוונה באשר להתמודדות עם איומי סייבר, וגורס כי להעלאה של רמת המודעות והמוכנות בנושאי הגנת סייבר באוכלוסייה הכללית יש חשיבות לאומית. רבות ממתקפות הסייבר מתחילות במחשבו הפרטי של מן דהוא. זה יכול להיות אזרח רגיל שמחשבו משמש כ-bot במתקפת DDOS, או עובד של ארגון כלשהו שחדירה לחשבונו מתחילה תהליך של privilege escalation שסופו חדירה ליעד המבוקש בארגון.

י. מטרת מסמך זה לקבוע תוכנית עבודה ותקציב מפורט להקמת מרכז תמיכה לאזרחים ועסקים קטנים למקרים של אירועי אבטחת סייבר (להלן – **המרכז**). הקמתו של המרכז תוקצבה עקרונית בתקציב 2016 של האיגוד, ומטרת מסמך זה לפרט את תהליכי הקמת המרכז והעלויות המרכזיות הנדרשות לצורך פעולתו.

2. תפישת העבודה להקמת המרכז

יא. האיגוד מקיים היום פעילות דומה, במישור הרעיוני, של "המרכז לאינטרנט בטוח" במסגרתו ניתן מענה 24X7 לאזרחים הפונים בסוגיות של אלימות ברשת, פרסום מידע פוגעני או אישי, הונאות רשת וכד'. המענה האנושי באירועים אלה נדרש מאחר והסוגיות שעולות הן בדרך כלל מאוד רגשיות, והתמיכה האנושית שהמרכז לאינטרנט בטוח מספק לגולשים עוזרת להם להתמודד עם החוויה השלילית הספציפית הקשורה בגלישה באינטרנט.

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי
ISOC-IL

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

יב. אירוע של הגנת סייבר הוא שונה במהותו, שכן לעיתים האדם כלל לא יודע שהוא יעד לתקיפת סייבר. במקרים רבים, המחשב פשוט אינו עובד טוב, או שקרה אירוע מוזר והאדם אינו יודע כיצד לפרש אותו.

יג. התובנה שהתגבשה באיגוד היא כי לא ניתן להעתיק את אופן הפעולה של מתן מענה אנושי הקיים במרכז לאינטרנט בטוח לאירועי סייבר, שכן המרכז עשוי להיות מוצף באלפי בקשות לעזרה טכנית בסוגיות טריוויאליות של תקלות מחשב. המענה לבעיות אלה עשוי להיות ארוך, וברוב המקרים נדרשת הגעתו של טכנאי לבדיקת המחשב על מנת לקבוע האם מדובר בבעיית חומרה, הגדרות מערכת הפעלה. תוכנה וכד'. בנוסף, בעוד שבסוגיות שבהן מטפל המרכז לאינטרנט בטוח יש לעיתים חשיבות קריטית בטיפול מיידי ואנושי (כגון באירועים בו מפורסמים חומרים אינטימיים על אודות אנשים או באירועים בהם יש חשש לכך שגולשים יפגעו בעצמם), בסוגיות הגנת סייבר, בדרך כלל, אין סיכונים מעין אלה.

יד. על כן, גובשה תפישת הפעלה המבוססת על מספר מודולים, שעיקרה מפורט להלן:

1. המודול הראשון שיסופק על ידי המרכז לאזרחים הוא אתר אינטרנט (להלן – **האתר**) המכיל מידע עדכני, אמין, בהיר ונגיש בסוגיות שונות של הגנת סייבר בצורת מדריכים (guidelines) בשפה ו/או אופן הצגה הברורה להדיוטות. במסגרת פעילות זו יופקו, לדוגמא, חומרי הסברה והדרכה לאזרחים כיצד לממש את "עשרת הדברות" בהגנה על מחשבם האישי.

2. המודול השני שיסופק על ידי המרכז לאזרחים יהא פורום אינטראקטיבי להעלאת בעיות באבטחת מידע ו/או תפעול המחשב על ידי אזרחים (להלן – **הפורום**), ומתן אפשרות לאחרים לסייע להם. פורום זה ינוטר באופן קבוע על ידי מנהל פורום מומחה אבטחת מידע מטעם האיגוד, אשר יוודא כי התמיכה הניתנת כעזרה הדדית אינה מטעה, מזיקה או זדונית. מקום בו לא תינתן תשובה בזמן סביר על ידי אחרים, יענה מנהל הפורום על הבעיה.

3. המודול השלישי שיסופק על ידי המרכז הוא מערך תקשור אפקטיבי (להלן – **רשת הפצה**) בשפה המובנת להדיוטות על אודות איומי סייבר עדכניים והדרך להתגונן מהם, כפי שמתגלים ומפורסמים על ידי ה-cert הלאומי הפועל במסגרת רשות הגנת הסייבר החדשה או מקורות אמינים אחרים. תקשור זה ייעשה הן באתר האינטרנט של המרכז, והן בדחיפה לצרכנים אשר נרשמו לקבלו (בדוא"ל, אפליקציה או בדרך אפקטיבית אחרת).

4. המודול הרביעי יבצע אסקלציה של בעיה נקודתית אצל אזרח שהועלתה בפורום

או שמידע על אודותיה הגיע ממקורות אחרים, כך שתעשה פניה ישירה לאותו גולש לבירור מעמיק של אירוע חשוד, אשר לא ניתן להסבירו ו/או לפותרו בתהליך פשוט וידוע (להלן – **הליך בירור**). תחילתו של הליך בירור תהא באספקה של פרטי מידע מהמחשב של הפונה (פרטי דוא"ל חשודים, קבצי תיעוד מערכת (log files), צילומי מסך וכד') לאתר מאובטח ונפרד במרכז לצורך בחינה. הבחינה תעשה על ידי מומחי אבטחת מידע ופורנזיקה מחברות אבטחת מידע מובילות, אשר יתרמו בנק שעות מומחה חודשי למרכז. העברת החומר תעשה על ידי עובדי המרכז לחברות.

5. המודול החמישי יתקיים בין המרכז ל-cert הלאומי. במסגרתו, יועברו חומרים חשודים, בין שאובחנו על ידי חברות אבטחת המידע כמתואר במודול הרביעי, ובין שהוחלט להעבירם ישירות ל-cert. חומרים אלה יבדקו וינותחו על ידי גופי המדינה העוסקים בנושא, וככל שידרש יווצר קשר ישיר בין גופי המדינה לאזרח שפנה, בין אם ישירות ובין אם דרך המרכז, לפי העניין.

טו. הסכימה הבאה מראה את התהליכים הנ"ל:

16. אתר המידע לציבור

יז. אתר המידע לציבור של המרכז ישתמש בשם מתחם ייעודי (כגון www.safe.org.il המשמש היום את המרכז לאינטרנט בטוח או www.isec.org.il) כך שניתן יהיה לקדם אותו באופן עצמאי ולפרסם את כתובתו לציבור הרחב.

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

יח. באתר יכללו השירותים הבאים:

1. סרטוני הדרכה ומדריכים כתובים לתהליכים מומלצים לשיפור אבטחת הסייבר של המחשב הטיפוסי לאזרח או לעסק הקטן. **דוגמאות**: הגדרה נכונה של משתמשים, שמירה על מערכת הפעלה מעודכנת, התקנת תוכנות הגנה (לרבות המלצות למוצרים חינמיים), גיבוי מידע וכד'.
2. סרטוני הדרכה ומדריכים כתובים לכללי התנהגות נכונים ברשת על ידי האזרח או העסק הקטן. **דוגמאות**: כיצד לזהות דוא"ל מזיק; כיצד לשמור על הפרטיות ברשת; כיצד שמור על מידע חשוב וכד'.
3. סרטוני הדרכה ומדריכים להתמודדות עם בעיות הגנת סייבר ידועות. **דוגמאות**: כללים להסרת נוזקה שהותקנה; כיצד להתמודד עם תקיפה ransomware מסויימות וכד'.
4. עדכונים על נוזקות חדשות ופרקטיקות תקיפת סייבר חדשות שאותרו.
5. האתר ישמש כשער הכניסה לפורום.
6. באתר ניתן יהיה להרשם לקבלת עדכונים אקטיביים (ב-push) בנושאים שונים של הגנת מידע וסייבר הרלוונטיים לציבור הרחב.

יט. אתר המידע יפותח על התשתית הכללית (WordPress) של אתר האינטרנט של האיגוד, כך שהתמיכה בו תוכל להתקיים בקלות על ידי צוות האיגוד.

כ. האתר יפעל בשתי שפות (עברית וערבית). לאתר תהיה גרסה אנגלית למטרות שיווק בינלאומי, אך החומרים לא יתורגמו לשפות אלה. החומרים יחוברו במקור בעברית, ויעשה להם תרגום (כתוביות, דיבוב או עיצוב מחדש והתאמה תרבותית – בהתאם לנושא ובהתאם למסקנות מהסקר שהאיגוד עורך בימים אלה) לערבית. תכנון החומרים יעשה תוך לקיחה בחשבון שהם אמורים להיות מופקים בשתי שפות (לדוגמא, אם מוצגים ממשק של מערכות הפעלה, תהינה גרסאות בעברית ובערבית).

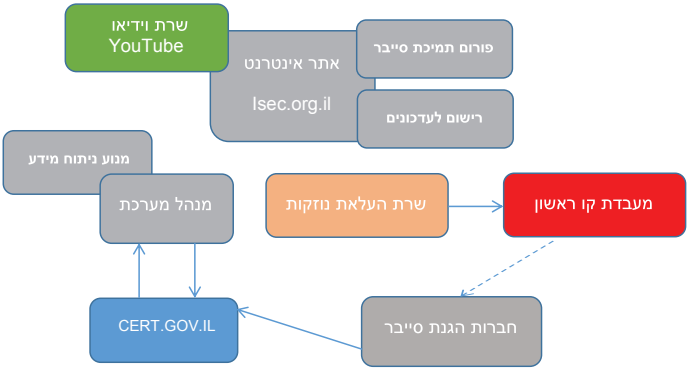
Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי
ISOC-IL

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

4. מערכות המידע הנדרשות לפעולת המרכז

כא. להלן מפת מערכות המידע הפועלות במסגרת המרכז או הקשורות לפעולתו.



כב. תפקידם העיקרי של מערכות המידע הנ"ל הוא:

1. **אתר אינטרנט** – משמש כשער הכניסה לכלל השירותים של המרכז וכפלטפורמה להעלאת תכנים שונים לידיעת האזרחים. האתר יעוצב כך שניתן יהיה לאתר בקלות מידע רלוונטי לפונים.

2. **פורום תמיכת סייבר** – פורום לניהול מערך החלפת המידע בין אזרחים לאזרחים אחרים, או בין המרכז לאזרחים לגבי שאלות ובעיות קונקרטיות שהועלו על ידי האזרחים במסגרת הפורום.

3. **שרת העלאת נוזקות** – שרת ייעודי מופרד ממערכות המרכז, אליו ישלחו אזרחים דוגמאות של נוזקות, או חומר מחשב החשוד כנוזקה. לשרת זה ניתן לשלוח דוא"ל או לעשות upload של המידע.

4. **שרת וידיאו** – שרת עליו יאוחסנו חומרי ההדרכה הויזואליים של המוקד. שרת זה יכול להיות שירות youtube, אך נדרשת יכולת ניתוח מאחדת בין השימוש בו ובין השימוש הכללי באתר.

5. **מעבדת קו ראשון** – מעבדה המאפשרת בדיקה מאובטחת ראשונית של הנוזקות שאותרו. מטרתה לאפשר הבנה ראשונית של הנוזקה, וגיבוש הגורם אליו יש להפנות את הנוזקה (חברות אבטחת מידע או רמת מדינה). המעבדה תהיה מנותקת מהאינטרנט וממערכות אחרות של המרכז ו/או האיגוד, כדי שלא יתאפשר דרכה לתקוף את האיגוד או את המרכז. החומר אליה יגיע בממשק חד-כיווני משרת העלאת הנוזקות.

6. **מערך רישום לעדכונים** – בסיס נתונים מאובטח לרישום פרטי אזרחים (שם וכתובת דוא"ל) לרשימת תפוצה לקבלת עדכונים בדחיפה (push) בנושאי הגנת סייבר.

7. **מנוע ניתוח מידע** – מנוע analytics שיפעל מעל הפורום והאתר ויזהה טרנדים בנושאים המעסיקים את הציבור בנושאי סייבר, כגון התקפות ספציפיות המופיעות אצל משתמשים שונים, אפיון הפונים, התנהגות הגולשים באתר וכד'. למנוע צריכה להיות יכולת text mining המאפשרת לנתח טקסט בעברית שמועלה על ידי משתמשים בפורום, כדי לבצע clustering אוטומטי של בעיות ותופעות.

8. **ממשקים** – למוקד יבנו ממשקים מאובטחים מול ה-cert הלאומי ומול חברות אבטחת מידע להעברה דו-כיוונית של מידע. מהמוקד יועברו שאלות וחומרים חשודים, מהחברות וה-cert יגיעו תשובות ועדכונים על נוזקות ואירועים שיש לתקשר לציבור.

5. כוח אדם

כג. בשלב ראשון לפעולת המרכז, ירכשו ממקורות חיצוניים עיקר משאבי כ"א הנדרשים לפעולתו. המשאב החשוב ביותר, וגם היקר ביותר, הוא הגורם אשר מנהל את הפורום ומתווה את התפיסה המקצועית של המענה לציבור (להלן – **מנהל הפורום**). לצורך זה מוצע, לפחות בשלב הראשון, להתקשר עם חברה המתמחה באבטחת סייבר ברמה גבוהה, ולקנות ממנה שירותי ייעוץ תוכן וניהול הפורום.

כד. תהליך הפקת החומרים יעשה בהתקשרות עם קבלני משנה המתמחים בהפקתה של חומרי הדרכה ממוחשבים. התוכן המקצועי יגיע ממנהל הפורום, בפיקוח ותיאום של כח האדם המקצועי באיגוד. עובדי האיגוד העוסקים בתחום הקשור לנושא (אורנה, נהורא) יפקחו על תהליך אספקת החומרים על ידי קבלני המשנה.

כה. במהלך שנת 2016 פעולת המרכז תפוקח ישירות על ידי המנכ"ל, שכן נדרשת תשומת לב ניהולית בכירה לתהליך הקמתו והתנעת פעילותו. עם התייצבותו של המרכז, ימונה לו מנהל מטעם האיגוד אשר יהיה אחראי לכלל פעילותו השוטפת. מנהל המרכז יהיה כפוף למנכ"ל.

כו. החל בפעולת מערך ה-cert המדינתי בבאר שבע (מוערך – יוני 2016), יפעל המרכז במבנה הסמוך אליו (WeWork). המטרה של הפעלה המרכז בסמוך ל-cert היא יצירת ממשק עבודה רציף מול אנשי ה-cert, **הן ברמה האנושית והן ברמה הטכנולוגית.**