סייבר ישראל
מערך הסייבר הלאומי

המלצות לאבטחת מידע וצמצום סיכוני סייבר לעסק קטן

יוני 2018

סייבר ישראל
מערך הסייבר הלאומי

המלצות לאבטחת מידע וצמצום סיכוני סייבר לעסק קטן

יוני 2018

מסמך זה נכתב ע"י מערך הסייבר הלאומי לטובת הציבור. המסמך מהווה המלצה לכלל בעלי העסקים במשק הישראלי. ניתן להשתמש בו לטובת העלאת החוסן בסייבר במשק באופן חופשי. מסמך זה נכתב עבור הציבור, בעלי העסקים, מיישמים ואנשי IT. המסמך מציג המלצות לאבטחת מידע לעסק הקטן. בהתאם לניתוח סיכונים שמבצע העסק ניתן לבנות תוכנית הגנה ולהוסיף המלצות בהתאם. המסמך פונה לכלל המשק ונכתב בלשון זכר מטעמי נוחות בלבד. התייחסות למסמך ניתן להעביר במייל tora@cyber.gov.il

כל הזכויות שמורות
למערך הסייבר הלאומי

מבוא

איומי הסייבר מהווים סיכון על החברה, לכלכלה ולמשק בישראל. ככאלו, הם מכוונים לכולם ואינם מבחינים בין ארגונים גדולים, או עסקים בינוניים וקטנים.

בשנים האחרונות ההתקפות המכוונות לארגונים במשק הינן תקיפות, המתבססות על טכנולוגיות ועל שיטות מתקדמות. פגיעת סייבר בעסק קטן עלולה לגרום לנזקים משמעותיים, כדוגמת מחיקת מאגרי מידע, נזקים תפעוליים, כספיים ותדמיתיים, ועד לשיתוק והשבתת הפעילות העסקית.
כיום, רמת האבטחה הממוצעת של ארגון קטן אינה מספקת אל מול איומי הסייבר ושיטות התקיפה. העסקים הקטנים מהווים נדבך חשוב במשק הישראלי וחשיבותם לכלכלה הישראלית גדולה, ובשל כך נדרשת העלאת חוסנו של הסייבר גם אצל אלו.
מטרת מסמך זה היא להנחות עסקים קטנים, ולהתוות עבורם את רמת ההגנה הבסיסית, שתסייע לצמצם את סיכוני הסייבר ולמזער את הנזקים. המסמך מתאים גם לעסקים אשר אינם מעסיקים אנשי אבטחת מידע באופן מלא. המסמך מציג את הצעדים הבסיסיים להגנה על מערכות המחשוב, המידע העסקי והלקוחות וניתן להשתמש בו כדרישות שניתן לדרוש מספקיות שירותיי ה-IT והמחשוב, והעובדים הטכניים בחברה.
יש לשים לב באם חלות חובות נוספות על העסק, מעצם היותו כפוף לרגולציות קיימות (כגון פרטיות, חומרים מסוכנים וכד').

המלצות לעסק הקטן

1. **מודעות עובדים** - תשומות והשקעה בתדרוך העובדים הינן הכרחיות. התקפות הסייבר נשענות לרוב על הנדסה חברתית וחולשות אדם, ובכך מאפשרות שיטוי והונאה של משתמש הקצה בארגון באופן שיאפשר התפשטות לשאר המחשבים. תוכנית הדרכה בשיתוף משאבי אנוש והקניית מודעות לעובדים מהוות נדבך חשוב, שתורם כמכפיל הכוח ולמניעת אירועי סייבר. כדוגמת תקיפה בהנדסה חברתית, הונאות פישינג או התקפת כופר ונעילת קבצים שעל המחשב וכד'.

לפרטים נוספים ראו בקרה 20.2 ובקרה 20.4 בתורת ההגנה בסייבר לארגון.

2. **מיפוי נכסי מידע וסקר סיכונים** - החיבור והקישוריות בין מחשבים, אפליקציות מובייל, שימוש בענן וכד' מגדילים את הזדמנויות התקיפה ואת "משטח התקיפה". **תהליך מיפוי יאפשר לזהות סיכונים קיימים לנכסי המידע ולמערכות המחשב של הארגון. זאת, בסיוע מומחה אבטחת מידע (מתוך הארגון או מחוצה לו) ובהתבסס על איומים ידועים, על חולשות במערכות ועל אמצעי אבטחה קיימים.** תהליך זה חיוני ומשפיע על הגדרת המדיניות של אבטחת המידע, **על התוכנית והתעדוף לטיפול בליקוי אבטחה ועל צמצום הסיכונים בפועל.** דוגמה למיפוי נכסי מידע וסקר סיכונים עבורו, למשל, בהקשר של מערכת סליקה מלקוחות, ובתוך כך - סקירה של אופן ביצוע הסליקה, רמת ההגנה על עמדת הסליקה (Point of Sale), אופן עיבוד המידע ומאגר הלקוחות, רמת הרשאות ומשתמשים וכד'.

לפרטים נוספים, ראו עמ' 19 מיפוי נכסים בתורת ההגנה בסייבר לארגון.[1]

טבלת מיפוי סיכונים מתוך תורת ההגנה בסייבר לארגון ראו בעמוד הבא.

3. **תוכנות ברישוי** - שימוש בתוכנות ברישוי מבטיח תהליך מסודר של עדכוני אבטחה. שימוש בתוכנות ללא רישוי או בתוכנות פרוצות מהווה הזדמנות אטרקטיבית לתוקף, בין היתר בשל העובדה שניתן לנצל חולשות בהעדר עדכוני אבטחה אחרונים. יש לוודא בתהליך הרכש הארגוני, הצטיידות והתקנת תוכנות ברישוי.

4. **אנטי-וירוס** - אנטי-וירוס היא תוכנה, המותקנת גם באופן מקומי על המחשב.[2] **מטרתה לאתר פוגענים באמצעות חתימות ידועות מראש.** וודאו מול אנשי ה-IT בארגון או מול ספקי שירותי המחשוב שתוכנת אנטי-וירוס תהיה מותקנת על כל המחשבים בעסק, כולל על השרתים, ושהתוכנה תתעדכן בתדירות גבוהה (לפחות פעם ביום). **תוכנת אנטי-וירוס**

[1] https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test

[2] תוכנה שנועדה לאתר וירוסי מחשב ולהגן על המחשב מפני פעילותם. ישנם גם אנטי וירוס מקוונים.

סוג הנכס	שם הנכס + יצרן	ייעוד הנכס	מקומי/ ענן	ממשקים	הערות
אפליקציה ארגונית					כגון ERP, CRM, DWH, WMS, מערכת שכר, פורטל ארגוני.
תשתית					כגון ציוד תקשורת, תשתית טלפוניה, דוא"ל ואחסון.
רשת					קווית ואלחוטית אופטית, לווייינית.
OT					יכול לכלול, לדוגמה, טלוויזיה במעגל סגור, מערכות HMI, בקרים ועוד.

טבלת מיפוי סיכונים מתוך תורת ההגנה בסייבר לארגון

עדכנית בהחלט יכולה למנוע פגיעה בעסק. קיימים מוצרים וסוגים שונים של אנטי-וירוס.[3]
לפרטים נוספים, ראו בקרה 7.3 בתורת ההגנה בסייבר לארגון.

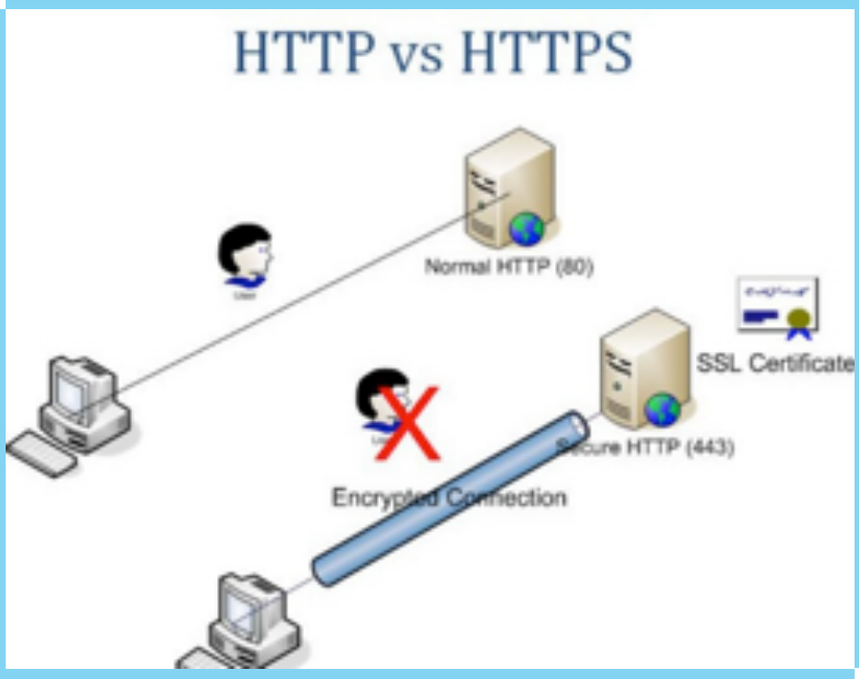
5. **עדכוני תוכנה** - על אנשי המחשוב להגדיר בכל התוכנות המותקנות עדכוני תוכנה אוטומטיים. הדבר קריטי במיוחד במערכת ההפעלה ובתוכנות שנעשה בהן שימוש רב (כדוגמת Office). עדכוני תוכנה יבטיחו, שהתוכנות המותקנות בעסק תהיינה תמיד מעודכנות בעדכוני האבטחה השונים, וכך תפחת משמעותית היכולת של תוקף פוטנציאלי לנצל חולשה באחת התוכנות ולתקוף את העסק.

למידע נוסף ראו בקרה 7.9 בתורת ההגנה בסייבר לארגון.

6. **סיסמאות הזדהות חזקות והגדרת נעילה לאחר כמה ניסיונות הזדהות כושלים** - אחד מערוצי התקיפה הנפוצים נשען על ניסיונות פריצה באמצעות ניחוש סיסמאות. התוקף מצויד במילון סיסמאות (Password Dictionary), המורכבות ממיליוני צירופים אפשריים. בעת תהליך התקיפה מתבצע תהליך הרצה של מילון הסיסמאות במטרה לנסות לנחש את הסיסמה. שימוש בסיסמה פשוטה מאפשר קלות ניחוש וגישה למערכות המחשוב. באמצעות צוות ה-IT הארגוני או ספקיות שירותי ה-IT והמחשוב, רצוי להגדיר סיסמה ארוכה וקשה לניחוש, המורכבת מצירוף של ספרות, אותיות גדולות וקטנות ותווים מיוחדים. שימוש במנגנון אימות דו שלבי יוצר רובד אבטחה ומענה טוב אל מול ניסיונות גניבת הסיסמאות גם בפישינג. פעולות פשוטות אלו יצמצמו את סיכוני התקיפה המבוססים על ניחוש סיסמאות.

[3] https://www.gartner.com/reviews/market/endpoint-protection-platforms

7. **הצפנת מידע כחלק משמירה והסתרה של מידע עסקי ונתוני לקוחות** - מטרת ההצפנה היא לשמור על חשאיות הנתונים מפני גורמים שאינם מורשים. פתרונות ההצפנה המקובלים נותנים מענה לשמירת המידע בתווך (כדוגמת דרישה מהספק לפתרונות HTTPS כפרוטוקול מאובטח) וכן לשמירת המידע באופן מוצפן גם בשרתים ובמחשבי החברה, נוסף על מעגלי אבטחה נוספים. תהליך ההצפנה המתבצע ע"י צוות ה- IT בארגון או באמצעות ספקית השירות מחייב הצטיידות בתוכנות מתאימות, ניהול מפתחות הצפנה וכד'.



8. **גיבוי** - תהליך **גיבוי מוסדר מאפשר יכולת התאוששות מתקיפות סייבר שונות.** הדוגמה הטובה ביותר היא מתקפת כופרה (Ransomware), שבה פוגען (Malware) מצפין את כל המידע הקיים על מחשב ספציפי או ברשת הארגונית. במקרה כזה ניתן לשחזר את המידע באמצעות גיבויים עדכניים ובכך למנוע פגיעה קשה יותר בעסק. קיימות שיטות גיבוי שונות - החל מגיבוי מקומי, גיבוי בענן או בהדפסה של עותק פיזי. ניתן לבצע גיבוי משולש שמטרתו לצמצם אובדן מידע בתהליך הגיבוי הראשוני או המשני. גיבויים יכולים להתבצע בצורה של דיסקים חיצוניים או קלטות, המחזיקים מידע קריטי של הארגון (ו**מיפוי נכסי המידע** הוא הדרך לזהות ולאתר מידע כזה). גיבויים יכולים להתבצע גם בצורה של אתר חלופי, שאליו עובר העסק במקרה אסון. חלופת הגיבוי תיבחר על פי אופיו הייחודי של העסק, בהתאם לרמת הקריטיות של חזרה מידית לעבודה וליכולת העסק להשקיע בפתרונות גיבוי שונים.

וודא מול אנשי ה-IT כי קיים תהליך גיבוי מתאים בהתאם להמלצות.

למידע נוסף, ראו בקרה 29.12 בתורת ההגנה בסייבר לארגון.

9. **רשתות אלחוטיות** - השימוש ברשתות אלחוטיות נפוץ מאוד בימים אלה הן לצורך הפעלת מערכות המחשב של העסק והן לצורך מתן שירות וגישה לאינטרנט עבור הלקוחות. בעת התקנה של רשת אלחוטית במשרד מומלץ להנחות את צוותי ה-IT להקפיד על הכללים האלה:

א. יש לקיים הפרדה מלאה בין רשת העסק

לרשת הלקוחות. מומלץ להקים שתי רשתות אלחוטיות שונות, כדי שלקוחות (או אלו המנצלים את השירות), לא יוכלו להשיג גישה לא מורשית למערכות העסק.

ב. יש לדרוש מספק התשתית את ההגדרות הבאות ברשת העסקית:

1) **הצפנה** - יש להשתמש באמצעי ההצפנה החזק ביותר (בזמן כתיבת שורות אלו WPA2).

2) **סיסמה** - יש להגדיר סיסמת רשת ארוכה ומורכבת ולהחליפה באופן עיתי.

3) **הקשחה על בסיס כתובות MAC** - מומלץ להקשיח ככל האפשר את כתובות ה-MAC המתחברות לנתב האלחוטי (כגון סינון White List).

4) **הסתרת שם רשת (SSID)** - יש להסתיר את שם הרשת כך שלא תהיה גלויה למי שסורקים רשתות אלחוטיות באזור.

5) **ניהול הנתב** - יש לשנות את סיסמת ברירת המחדל לניהול הנתב.

ג. מומלץ לבחון מענה הצפנה לרכיבים אלחוטיים נוספים (כדוגמת מקלדת אלחוטית, עכבר אלחוטי, מדפסת אלחוטית וכד').

10. **ביטוח סייבר** -למרות כל מנגנוני ההגנה הקיימים, מתקפות סייבר עדיין מצליחות לפגוע בעסקים. הדרך למזער את הנזק הכלכלי ממתקפה מוצלחת היא רכישת ביטוח סייבר, שישפה את העסק במקרה של פגיעה כלכלית כתוצאה ממתקפת סייבר. יש לזכור, כי בדומה לכל ביטוח אחר, גם ביטוח סייבר מחייב את העסק ליישם רמה בסיסית של הגנה כדי שיהיה זכאי לפיצוי. מעבר למזעור הנזק הכלכלי, תהליך זה יסייע בהתאוששות מאסון ובשרידות עסקית.

האם העסק שלך מוגן?

ריכוז ההמלצות לאבטחת מידע וצמצום סיכוני סייבר לעסק הקטן

המלצות	אופן מימוש	תדירות	נוסף
מודעות עובדים	תוכנית הדרכה, דף הנחיות, דואר אלקטרוני, פוסטרים ברחבי העסק.	ככל שהתדירות עולה כך עולה מודעות העובדים. התדירות המינימלית היא אחת לשנה.	ניתן להיעזר בחברות המתמחות בקמפיין מודעות עובדים.
מיפוי נכסי מידע וסקר סיכונים	ראיון עם כלל הגורמים בחברה לאיתור נכסי המידע של העסק וביצוע סקרי סיכונים שמטרתם להצביע על אזורים חלשים בהם נדרשת הגברת אבטחה.	יישור קו חד-פעמי, ולאחר מכן עדכון על בסיס שנתי.	מומלץ להכין שאלון מראש. ראו טבלת מיפוי סיכונים במסמך עמ' 5
תוכנות ברישוי	יש לבחון שכל התוכנות בעסק הינן ברישיון הרלוונטי לעסק - כחלק מתהליך מבטיח לעדכוני אבטחה.	סקר איתור תוכנות חוקיות נעשה באופן חד-פעמי, ולאחר מכן כל תוכנה חדשה חייבת להירכש עם רישיון חוקי.	מומלץ לייסד נוהל עבודה לרכש תוכנה על מנת לוודא, שכל העובדים בארגון מודעים לחשיבות השימוש בתוכנות חוקיות ופועלים בהתאם.
אנטי-וירוס	יש להגדיר עדכונים אוטומטיים בפתרון האנטי-וירוס של העסק.	בהתאם לניהול הסיכונים וצרכי הארגון או בהתאם להמלצות היצרן.	
עדכוני תוכנה	העדיפות הגבוהה ביותר היא למערכת ההפעלה. כל מערכות ההפעלה כוללות אפשרות לעדכונים אוטומטיים. מומלץ לוודא שכל מערכות המחשוב בעסק אכן מוגדרות כך במטרה להבטיח תהליך של סגירת טלאי אבטחה.	יש לבחון עדכונים אוטומטיים אל מול עיתיים.	מרבית התוכנות מוגדרות אוטומטית לעדכון עדכונים מיצרן התוכנה.

ריכוז ההמלצות לאבטחת מידע
וצמצום סיכוני סייבר לעסק הקטן - המשך

המלצות	אופן מימוש	תדירות	נוסף
סיסמאות הזדהות חזקה	מומלץ להיעזר ביועץ אבטחת מידע או באינטגרטור למערכות הזדהות חזקות ליצירת מדיניות סיסמאות מתאימה ושילב מנגנון אימות דו שלבי כנגד ניסיונות פישינג לגניבת סיסמאות.	הקמת מערכת הזדהות חזקה נעשית באופן חד-פעמי.	
הצפנת נתונים	יש לבצע בדיקה ולוודא כי תעבורת מידע רגיש ושמירתו מתבצעת בפלטפורמה מוצפנת.	הערכת סיכונים ביחס לרגישות הנתונים בכול שילוב של יישום, אפליקציה או תוכנה חדשה .	
גיבויים	אופן הגיבוי תלוי בנפח המידע המגובה ובתדירות הנדרשת. ניתן לבצע בשיטות שונות כגון גיבוי קר או חם באופן שיאפשר שיחזור ונגישות למידע במידת הצורך.	תדירות הגיבויים תלויה ברמת הקריטיות של המידע המגובה.	מומלץ להיעזר ביועץ מומחה לנושא גיבויים והתאוששות מאסון.
רשתות אלחוטיות	יש להנחות את ספק האינטרנט או הנתב להקשחה בסיסמאות.	הגדרות ראשוניות באופן חד פעמי. סיסמאות יש להחליף אחת לשנה.	מומלץ לשמור את הסיסמאות בעותק קשיח במקום מוגן.
ביטוח סייבר	ככיסוי נוסף אל מול אירועי הסייבר, שרידות עסקית ויכולת התאוששות מאסון.		

סייבר ישראל
מערך הסייבר הלאומי

119
tora@cyber.gov.il
www.cyber.gov.il

חפשו אותנו