מדיניות

להגנת מידע וסייבר

באיגוד האינטרנט הישראלי

תוכן עניינים

1. רקע

1.1. מרחב הסייבר הוא תולדה של קדמה טכנולוגית, קישוריות וחיבור גלובלי לרשת האינטרנט.

1.2. התלות הגוברת במרחב הסייבר מביאה עמה בשורות של חדשנות טכנולוגית ופיתוחים אדירים לאדם ולסביבתו.

1.3. לצד אלה מתפתח מרחב איומים, המשפיע על הרציפות התפקודית הארגונית, על שלמות תהליכי העבודה ועל סודיות המידע של איגוד האינטרנט הישראלי (להלן "האיגוד" או "איגוד האינטרנט").

1.4. מתקפות סייבר עלולות לפגוע בארגונים ואף להביא להפסקת תהליכי העבודה, לנזק כלכלי ולפגיעה במוניטין של האיגוד.

1.5. איגוד האינטרנט הינו מנהל ה-(ccTLD (Country Code Top Level Domain של מרחב IL., וככזה מנהל את מרשם שמות המתחם של המתחם ומפיץ את מידע ה-DNS לגביו. בנוסף, מפעיל האיגוד את מחלף האינטרנט הישראלי IIX, המקשר בין רוב ספקי הגישה לאינטרנט בישראל. בנוסף, הארגון מנהל פעילות ענפה של קידום מדיניות ציבורית בסוגיות של הטמעת השימוש באינטרנט בחברה הישראלית.

1.6. פעילותו התקינה של איגוד האינטרנט מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות והשרידות של מערכות המחשוב והתקשורת המופעלות בו, והמידע אותו הוא מפיץ.

1.7. המידע, מערכות התקשוב המעבדות ומאכסנות אותו, אמצעי התקשורת והאמצעים והציוד הנוספים המשמשים לפעולת האיגוד (להלן "נכסי המידע"), מהווים נכס מרכזי וחיוני לאיגוד ויש להגן עליהם ברמה הטובה ביותר.

1.8. פגיעה בנכסי המידע עשויה לפגוע באופן מהותי בשירותים אותם מספק האיגוד, ובכך לפגיעה בגופים המסתמכים על שירותי האיגוד, לאובדן כספים, לפגיעה בצנעת הפרט של לקוחות ו/או עובדים, לפגיעה במוניטין ובתדמית האיגוד.

1.9. המדיניות להגנת הסייבר באיגוד מבוססת על ניתוח הסיכונים לנכסי המידע תוך התאמה לצרכים התפעוליים והארגוניים של האיגוד. העקרונות המונחים במדיניות להגנת הסייבר באיגוד מהווים בסיס לנהלי העבודה בתחום הגנת הסייבר.

1.10. המדיניות להגנת הסייבר באיגוד נגזרת, בראש ובראשונה, מרגישות השירותים שהאיגוד מספק למשתמשי האינטרנט בישראל, וכן מחוקים, תקנות והנחיות בהם מחויב האיגוד והעובדים בה לעמוד, לרבות תקן ניהול "אבטחת המידע" הבינלאומי ISO 27001.

1.11. מדיניות להגנת הסייבר באיגוד כורכת בתוכה את הנחיות המסגרת להגנת הסייבר באיגוד, כנספח למדיניות.

2. מקורות עליהם נסמכת המדיניות

2.1. RFC של IETF לניהול מערכי מרשם שמות מרשם והפצת DNS.

2.2. תורת ההגנה הלאומית של הרשות הלאומית להגנת הסייבר.

2.3. חוק הגנת הפרטיות, התשמ"א-1981 והתקנות הנלוות.

2.4. תקן ניהול "אבטחת המידע" ת"י ISO 27001.

2.5. חוקים, תקנות, הנחיות והתחייבויות נוספים שהאיגוד מחויב לעמוד בהם.

3. תכולה

3.1. המדיניות והנחיות המסגרת תקפים לכלל המתקנים ועובדי האיגוד, ובכלל זה עובדים פנימיים (קבועים וזמניים), עובדי מיקור חוץ (OUTSOURCING), עובדי קבלן בעלי נגישות למידע השייך ו/או הנוגע לאיגוד, בתוך האיגוד ובכל היחידות הארגוניות הכלולות במבנה הארגוני של האיגוד.

4. הגדרות

4.1. **סייבר – המרחב הקיברנטי**: מרחב הסייבר מורכב מארבעה רבדים:

1) **רובד פיזי**: כלל רכיבי המחשוב והתקשורת – מעבדים, מחשבים, נתבים, מתגים וכו'.
2) **רובד לוגי**: הקוד המפעיל את רכיבי המחשוב וקובע כיצד יפעלו.
3) **רובד מידעי**: פריטי מידע בפורמט דיגיטלי הנאגרים ברובד הפיזי ומיושם עליהם רובד לוגי.
4) **רובד אנושי**: כלל האנשים המשתמשים בשלושת הרבדים – פיזי, לוגי ומידעי.

4.2. **הגנת סייבר**: תחום שעניינו להגן על נכסים ברבדים הפיזי, הלוגי והמידעי במרחב הסייבר מפני תקיפות המכוונות לגנוב מידע, לשבש את פעולת מערכות המידע או

לפגוע בהן פיזית, לגנוב את המערכות או להשתלט אליהם, לשבש או לסכל את היכולת של המערכות לתפקד כהלכה ולמנעו מהן למלא את משימתן.

הגנת סייבר כוללת תהליכי איסוף מודיעין על יריבים פוטנציאליים, שימוש בכלי סייבר כדי לאתר "פוגענים" ו"נוזקות" שכבר נכנסו למערכת ונמצאים בתוכה, ניטור של המידע העובר ברשת וחיפוש אחרי אנומליות ו/או תקשורת בין "סוסים טרויאניים" למרכיב ה"פיקוד ושליטה" שלהם וכדומה.

תחום זה כולל גם "הגנה אקטיבית", כלומר פעילות שתכליתה לזהות תוקפים, תקיפות וזליגת מידע על ידי ניטור והפעלת כלי תקיפה על מערכות שעליהם מתכוונים להגן.

4.3. **מדיניות להגנת הסייבר**: עקרונות המפורטים במסמך זה מטעם הנהלת האיגוד בו מגדירה ההנהלה לגבי מחויבות העובדים לעמידה בחוק, בתקנות ובהנחיות הגופים הרגולטוריים ועל פי תקן ישראלי ISO 27001 בהיבט סיכול איומי סייבר והגנה על המידע באיגוד.

4.4. **מידע**: כל נתון המשמש, נוגע ו/או הקשור לפעילותו, תפעולו או תפקודו של האיגוד, לרבות מידע הנוגע לצנעת הפרט ומידע אישי רגיש, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, מצעי מידע פיזיים וכן מידע המועבר בעל-פה.

4.5. **ועדת ההיגוי לשירותי התשתית של האיגוד –** ועדת היגוי המורכבת משלושה נציגי ציבור, שני חברי וועד מנהל של האיגוד, מנהל התשתיות ומנכ"ל האיגוד, המנחה ומבקרת את פעילות מרכז התשתיות של האיגוד.

4.6. **ועדת ההיגוי לנושא הגנת הסייבר**: פורום ניהולי בראשות יו"ר ועדת ההיגוי לשירותי התשתית של האיגוד, הכולל את חברי וועדת ההיגוי לשירותי התשתית של האיגוד ונציגים בכירים באיגוד בעלי אחריות לתחום הגנת הסייבר, לרבות אחריות בהיבטים טכנולוגיים, אבטחתיים, תפעוליים, תקציבים, משאבי אנוש, יועץ משפטי ונציגים נוספים לפי שיקול דעתו של היו"ר.
הועדה נועדה לאשרר ולתקף את רמת הגנת הסייבר של האיגוד, מדיניות האיגוד בתחום ההגנה על הסייבר, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.
הוועדה תתכנס לכל הפחות פעם בשנה.

5. מטרות המדיניות להגנת הסייבר באיגוד

5.1. צמצום הסיכונים העלולים להוביל לפגיעה בנכסי המידע של האיגוד.

5.2. מזעור סיכוני הפגיעה בפעילות הסדירה של האיגוד.

5.3. עמידה בחוקים ובתקנים אליהם מחויב האיגוד והעובדים.

5.4. הצגת תפיסת הנהלת האיגוד לגבי הגנת הסייבר ומחויבותה לנושא.

5.5. קביעת עקרונות מנחים ליישום הגנת הסייבר באיגוד, על בסיסם ניתן יהיה ליישם אמצעי אבטחה ולאורם ניתן יהיה לבחון את רמת האבטחה הקיימת.

5.6. העלאת רמת המודעות של מנהלי האיגוד ועובדיו לנושאי הגנת הסייבר.

5.7. הגדרת סמכויות הגנת הסייבר באיגוד.

5.8. מתן מסגרת לתהליכים המרכזיים באיגוד בנושאי הגנת הסייבר, תוך יצירת תשתית לנהלים מקיפים.

5.9. ביצוע תהליכי שיפור מתמיד בנושאי הגנת הסייבר באיגוד.

6. עיקרי המדיניות להגנת הסייבר באיגוד

6.1. מבנה ארגוני

להגדיר את המסגרות הארגוניות, אשר יישמו את המדיניות להגנת הסייבר באיגוד ויבקרו את אופן יישומה. בפרק זה יוגדרו בעלי התפקידים השונים, וכן יפורטו סמכויותיהם ויחסי הגומלין ביניהם.

6.2. אבטחה פיזית

הגנה על מכלול הציוד והמידע המצויים באתרי האיגוד מפני גישה פיזית של גורמים בלתי מורשים, אשר תוצאותיה עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע.

6.3. אבטחת רשומות

הגדרת תהליכי וכלי הטיפול ברשומות (מצעים פיזיים נושאי מידע), במטרה לצמצם את סיכוני הפגיעה במידע האגור בהם.

6.4. הגנה לוגית

הגדרת שכבות האבטחה בתחומים הלוגיים, המהווים מעגלי הגנה על המידע, בתחומי המחשוב והתקשורת (להלן ה"תיקשוב").

6.5. אבטחת משאבי אנוש

קביעת עקרונות אבטחת מידע בכל הקשור לעובדי האיגוד (עובדים פנימיים, קבועים וזמניים, עובדי מיקור חוץ - OUTSOURCING), תהליכי הקליטה והעזיבה של עובדים, על מנת לצמצם את הסיכונים הנובעים מחוסר מודעות של עובדים, טעויות אנוש, התנערות מאחריות או רצון מכוון של עובד לפגוע בנכסי המידע של האיגוד.

6.6. ניהול וסיווג נכסים

להבטיח כי כל נכסי המידע באיגוד ידועים, מסווגים ומנוהלים כראוי, וכי קיים גורם הנושא באחריות לגבי כל אחד מנכסי המידע.

6.7. אבטחת ממשקים עסקיים - שרשרת אספקה

צמצום הסיכונים הנובעים מחשיפה של עובדי חברות חיצוניות למידע ולמערכות של האיגוד.

6.8. טיפול באירועי הגנת הסייבר

קביעת עקרונות דיווח וטיפול באירועי הגנת הסייבר, באמצעותם ניתן יהיה לצמצם את הנזק שיגרם כתוצאה מהאירועים, תיקון הליקויים, טיפול משמעתי בגורמים הרלוונטיים והפקת לקחים לעתיד.

6.9. פיתוח ורכש

לקבוע עקרונות לשילוב אבטחת הסייבר ומידע בתהליכי הפיתוח והרכש, על מנת להבטיח כי יושמו במערכות המידע של האיגוד אמצעי אבטחה מתאימים, בהתאם לרמת הרגישות של כל מערכת.

6.10. ניהול המשכיות עסקית

הגדרת העקרונות שיאפשרו את המשך פעילות המחשוב העסקית והחיונית של האיגוד בעת חירום.

6.11. תוכנית עבודה ותקציב

גיבוש תכנית העבודה והתקציב בתחומי הגנת הסייבר באיגוד, במטרה לעמוד ביעדים ולנתב משאבים נדרשים.

6.12. הטמעה

וידוא כי מדיניות זו, והכללים הנגזרים ממנה, יוטמעו באופן משמעותי בתרבות הארגונית של האיגוד ובעובדיו.

6.13. התאמה (COMPLIANCE)

להבטיח כי האיגוד עומדת בכל דרישות החוק הישראלי, הנוגעות להיבטי הגנת הסייבר. הגדרת הפעילויות, הכלים והאמצעים, אשר ישמשו את גורמי הגנת הסייבר לבדיקת היישום של מדיניות הגנת הסייבר באיגוד, הנהלים והסטנדרטיים הטכניים במערכות השונות ובקרב עובדי האיגוד.

הגנת הסייבר באיגוד תיושם בכפוף ובצמידות לחוקי מדינת ישראל הנוגעים לתחום אבטחת המידע, לרבות חוזרים, נהלים והנחיות של הגורם המנחה, תורת ההגנה הלאומית של הרשות הלאומית להגנת הסייבר, חוק הגנת הפרטיות, התשמ"א-1981 והתקנות הנלוות; תקן ניהול "אבטחת המידע" ת"י ISO 27001.

7. אחריות על מדיניות הגנת הסייבר

7.1. ועדת ההיגוי לנושא הגנת הסייבר באיגוד אחראית לגיבוש עקרונות המדיניות, להתוויית אסטרטגיות לפעילות, לפיקוח אחר תכנית האב ותכניות העבודה השנתיות, לווידוא הטמעתו בתרבות הארגונית של האיגוד, לקיום הערכת נזקים בעקבות תקלות ולגיבוש המלצות לטיפול על פי עקרונות מסמך המדיניות והמסגרת להגנה על הסייבר.

7.2. ממונה הגנת הסייבר אחראי לניהול והנחייה מקצועית שוטפת בתחום הגנת הסייבר והנחלה בשטח של החלטות וסיכומי ועדת ההיגוי להגנת הסייבר.

7.3. ממונה הגנת הסייבר אחראי לעדכון מסמך זה עפ"י הצורך.

8. בקרה

8.1. ועדת ההיגוי לנושא הגנת סייבר באיגוד תבצע סקירה של ישימות מדיניות הגנת הסייבר במסגרת סקר הנהלה על פי מתווה הנחיות המסגרת להגנת הסייבר.

8.2. ועדת ההיגוי לנושא הגנת סייבר באיגוד תאשר במסגרת סקר ההנהלה פרמטרים לבדיקת אפקטיביות של מערך הגנת סייבר באיגוד. הפרמטרים יכללו מדדים כמותיים לבחינת רמת העמידה בפרמטרים המוגדרים.