מדיניות אבטחת מידע

גלופת לימוד

מדיניות האבטחה בארגון היא הבסיס לכל פעילות האבטחה בו. עיצוב או הגדרה של מדיניות אבטחת מידע הינם תהליך, ואינם פעולה חד פעמית של כתיבת מסמך.

תהליך זה כולל שני שלבים עיקריים, העוסקים בשתי רמות שונות של המדיניות עקרונות אבטחת מידע כלליים ומדיניות מפורטת

תוכן העניינים

1. כללי 2
2. עקרונות אבטחת מידע כלליים 2
3. מדיניות מפורטת 2

©
נוהל מפת״ח הוא מוצר המוגן בזכויות יוצרים
הזכויות במגזר הממשלתי הן של משרד האוצר
הזכויות מחוץ למגזר הממשלתי הן של מתודה מחשבים בע״מ
זכויות השימוש של רוכשי הנוהל הן בהתאם לרישוי שברשותם.

1. כללי

מדיניות האבטחה בארגון היא הבסיס לכל פעילות האבטחה בו. עיצוב או הגדרה של מדיניות אבטחת מידע הינן תהליך, ואינן פעולה חד פעמית של כתיבת מסמך. לרוב, תהליך זה כולל שני שלבים עיקריים, העוסקים בשתי רמות שונות של המדיניות:

- עקרונות אבטחת מידע כלליים
- מדיניות מפורטת

2. עקרונות אבטחת מידע כלליים

שלב ראשוני זה כולל הגדרת עקרונות ברמה גבוהה, הנובעים מעקרונות בסיסיים ארגוניים, כגון מדיניות עסקית, תחרותיות בשוק, מדיניות לשרידות, רגולציות מטעם החוק או מגופים מנחים, וגם מהגיון בריא.

ברמה זאת של מדיניות אין התייחסות לפרטי סביבת המחשוב בארגון או לסיכונים ספציפיים, ואין ירידה לפרטים.

להלן דוגמאות של נושאים הכלולים בחלק זה של המדיניות:

- איסור העברת מידע רגיש אודות הארגון לגורמים בלתי מורשים, מתחרים או עוינים
- הצורך במנגנוני זיהוי ואימות הזיהוי עבור כל משתמש במערכות המחשוב
- איסור הכנסת אמצעי זיכרון חיצוניים למחשבי הארגון ללא אישור ובדיקתם לפני כן
- איסור הוצאת מידע ממחשבי הארגון למחשבים חיצוניים
- הצורך ברישום כל אירוע חריג בשימוש במערכות המחשב בארגון
- כיבוי מחשבים בסוף היום ואחסון של מצעי זיכרון בהתאם לרגישות המידע האגור בהם
- דווח מיידי לאחראי על אבטחת המידע בארגון על כל חשד לעבירה או תקלת אבטחת מידע

3. מדיניות מפורטת

בשלב זה של הגדרת המדיניות קיימת התייחסות מפורטת לסביבת המחשוב בארגון, לתהליכים הארגוניים הממוחשבים, ולסיכונים הספציפיים הנובעים מאותם הסביבות והתהליכים הממוחשבים. תהליך מקדים להגדרת המדיניות המפורטת הינו ביצוע של סקר אבטחת מידע (סקר סיכונים).

סקרי אבטחת מידע תקופתיים עשויים לגרום לעדכון של מדיניות אבטחת המידע, בעיקר של המדיניות המפורטת.

להלן מספר דוגמאות של מדיניות מפורטת:

- בניית ארכיטקטורת רשת מאובטחת בהתאם לאיומים הרלבנטיים
- ביצוע הקשחה של השרתים בארגון
- ביצוע הקשחה של רכיבי התקשורת (נתבים, מתגים וכד')
- התקנת שני סוגי אנטי וירוס, אחד לשרתים והשני לתחנות הקצה

©
- כל הזכויות שמורות לממשלת ישראל וחברת מתודה מחשבים בע"מ -
- www.methoda.co.il -

- התקנה שוטפת של עדכוני תוכנה הקשורים לאבטחה עבור תוכנות תשתית, כגון מערכות הפעלה, דפדפן, שרתי דואר וכד'
- שימוש במוצר להצפנת תעבורת האימייל מול ספקים רגישים
- מדיניות לגבי סוג האימות של המשתמשים (סיסמה, כרטיס חכם וכד')
- נטרול של כונני הדיסקטים וכונני ה-CD במחשבים
- אוסף הנחיות של מותר ואסור עבור השימוש במחשב נייד
- שימוש במנגנוני אבטחה באפליקציות ומסדי נתונים

©
- כל הזכויות שמורות לממשלת ישראל וחברת מתודה מחשבים בע"מ -
- www.methoda.co.il -