סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

שאלות מיקוד עבור קובעי מדיניות בתחום הסייבר

כבעלי תפקיד ניהולי בחברה, הנכם מובילים ומשפיעים על אסטרטגית הארגון ועל החלטות משמעותיות לתפקודו. בין נושאי קבלת ההחלטות והתוויית המדיניות נכלל גם תחום ההגנה בסייבר.
מסמך זה פורס בפניכם את השאלות הבסיסיות ביותר, מומלץ לוודא כי מתקיים בהן דיון מעמיק באופן עיתי. המסמך מתייחס לשאלות אסטרטגיות המסייעות להגדרת סיכוני הסייבר של הארגון והמענה הרצוי בהתאם. המענה המצופה מבעלי תפקיד מופיע בפירוט בתורת ההגנה הארגונית של מערך הסייבר הלאומי.
אנו ממליצים לכל בעל תפקיד בכיר לעיין במסמך זה.

1. **האם הנהלת הארגון הגדירה מהם הנכסים ו/או התהליכים העסקיים הקריטיים ביותר לארגון? כיצד אירוע סייבר עלול להשפיע על נכסים/תהליכים אלו?**

מטרת ההגנה בסייבר הינה לאפשר לארגון לפעול במרחב הסייבר ללא חשש לפגיעה ברציפות התפקודית ובמוניטין, ולמזער נזקים פוטנציאלים אשר הארגון חשוף להם כתוצאה מהתלות במרחב זה. הגדרת ליבת הפעילות והתשתית הטכנולוגית המאפשרות השגת מטרות אלו, תסייע למקד את המאמצים במקומות הנכונים בארגון.

2. **מהי רמת ההשקעה של הארגון בהגנה בסייבר ועד כמה הארגון מוגן? האם הוגדרו מדדי ביצוע בתחום הסייבר בארגון (Key Performance Indicators)? כיצד מדידה זו מתבצעת בארגונך? כלים אוטומטיים שונים מאפשרים להציג את רמת הבשלות של הארגון. לשימושך, החל מ־Q3/2018 מדידה זו תוכל להתבצע בפשטות וללא עלות באמצעות מערכת יוב"ל של מערך הסייבר הלאומי**

ללא מדידה של רמת ההגנה, לצד הגדרת יעדים מדידים, ניהול ההגנה מתבצע תחת מעטה של ערפל. הגדרת היעדים והמדדים תסייע לתאם ציפיות בין הנהלת הארגון לממונה על ההגנה בסייבר בארגון ותאפשר צפייה במגמות לאורך ציר הזמן.

3. **מהם סיכוני הסייבר המהותיים לארגון? האם סיכונים אלו דורגו ושוקפו להנהלה באמצעות "מפת חום" ארגונית?**

לכל מגזר עסקי אופייניים סיכוני סייבר מסוימים וקיימים סדרי עדיפויות הרלבנטיים למגזר. כך, סיכוני הסייבר של בית חולים יהיו שונים מסיכוני חברת מזון. אף בין בתי החולים השונים, ייתכנו שינויים בראיית הסיכון בעיני ההנהלה. קיום דיון מעמיק על ההסתברות להתממשות סיכונים אלו ועל הנזק הפוטנציאלי במידה ואכן יתממשו, יסייע ליצירת אסטרטגיית הגנה רלבנטית.

4. **על איזו מתודה נשענת הגנת הסייבר של הארגון? האם סטנדרט זה כולל התייחסות ליכולת לאתר אירוע ולהגיב לו (Detect & respond)? מהי רמת ההגנה הארגונית אל מול דרישות תורת ההגנה בסייבר הלאומית?**

הישענות על מתודה סדורה, אשר מבוססת על ניסיונם של ארגונים רבים, תורמת לבניית תכנית עבודה וריכוז מאמצים בצורה אפקטיבית יותר.

5. **האם מצוי בידי הארגון המידע הדרוש לטובת קבלת החלטות וגיבוש האסטרטגיה בנושא הסייבר?**

ערוץ מוסדר מול הגורם אשר אמון על נושא ההגנה בסייבר בארגון מסייע לקבל תמונת מצב עדכנית. סקירה עיתית בנושא ע"י הגורם הרלוונטי בארגון מסייעת להציף דברים "מהשטח" לצד אפשרות לתשאל באופן ישיר את הגורם המטפל בנושא בשגרה.

6. **כיצד הארגון מגן על מידע שנמצא אצל ספקים וקבלני משנה? האם ישנה מתודה סדורה להגנה מפני אירוע סייבר שמקורו בשרשרת האספקה?**

שרשרת האספקה מהווה אחד מהאיומים הגדולים ביותר בתחום הסייבר. תקיפות רבות מגיעות אל הארגון דרך תקיפת שרשרת האספקה שלו. כמו-כן, פעמים רבות אירוע סייבר אצל ספק אשר הוצאנו אליו מידע עסקי רגיש, או אשר אפשרנו לו גישה מרחוק אל המערכות שלנו, חושף אותנו לסיכונים אשר השליטה עליהם מוגבלת. יש לקבוע מדיניות לעבודה נכונה עם ספקים וקבלני משנה בהיבטי הסייבר, תוך מיקוד בסיכון הסייבר וכיסוי היבטים משפטיים רלוונטיים.

7. **לאילו חוקים ורגולציה בתחום הסייבר הארגון כפוף ומהי מידת העמידה בדרישות אלו? האם רגולציה זו כוללת חובת דיווח על אירועי סייבר?**

על הארגון למפות לאלו חוקים ותקנות הוא נתון כתוצאה מפעילותו העסקית. מיפוי זה מסייע להפחית את הסיכון לסנקציה פלילית ו/או כלכלית מצד רגולטורים ותובעים פוטנציאלים.