14 בנובמבר, 2019

עיקרי הנחיית יה"ב -5.19

ניהול ספקים בשרשרת האספקה של משרדי הממשלה ויחידות הסמך

1. מקור הסמכות

החלטת הממשלה מספר 2443, מיום 15 פברואר 2015, קבעה כי ייעוד היחידה להגנת הסייבר בממשלה (יה"ב) הינו הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך. הנחיות יה"ב מחייבות את משרדי הממשלה ויחידות הסמך.

2. קהל היעד

בעלי התפקידים הבאים במשרדי הממשלה ויחידות הסמך-
ממוני הגנת סייבר, מנהלי מערכות מידע ומנהלי אבטחת מידע והגנת סייבר.

3. מטרת ההנחיה בנוסחה המלא

3.1. הנחיית קהל היעד בדבר ניהול יעיל של מערך אבטחת המידע ומזעור איומי הסייבר אשר מקורם בשרשרת האספקה לצורך העלאת החוסן של המשרד כנגד תקיפות סייבר.

3.2. הצגת מתודה סדורה של השלבים השונים בתהליך מובנה של ניהול סיכוני הסייבר בעת התקשרות עם הספק.

3.3. הנגשת נוהל עבודה רוחבי בעל תוכן מחייב את משרדי הממשלה ויחידות הסמך.

4. האיום

בחינה שנעשתה במשק הישראלי בשנת 2018, העלתה תמונת מצב, לפיה העדרם של תקן/שפה מקובלים של ארגונים במשק אל מול הספקים שלהם יוצרים קושי בקרב הארגונים ודורשים השקעת משאבים בפיתוח ותחזוקת הפעילות מול הספק. בנוסף, משרדים אינם מצליחים לנהל את היקף הבקרות על הספקים ולתקפם.

5. אחריות המשרד

5.1. על המשרד מוטלת האחריות לוודא, כי הספק מיישם את התהליך הנדרש כתוצאה מהנחיה זו וכמו כן לבצע בחינת עמידות לספק בהתאם לדרישות שהוגדרו, במיוחד כאשר הספק מוגדר כספק מהותי.

5.2. המשרד ימנה בעל תפקיד האחראי על שרשרת האספקה במשרד (להלן ממונה שרשרת אספקה), אשר יהווה איש קשר למיפוי הספקים ודירוגם, כמוכן, יהווה כתובת במשרד לפניות בנושא זה.

5.3. על המשרד לוודא כי קיים איש קשר מצד הספק אשר ידע לתת מענה בנושאים הרלוונטיים.

5.4. על המשרד לוודא כי לספק קיימות יכולות ניטור אירועי אבטחת מידע שיועברו לידיעת המשרד.

5.5. מידע אשר יוגדר ע"י המשרד כמידע תפעולי רגיש יועבר לספק בתצורה מאובטחת בלבד (דוא"ל מוצפן) או באמצעות מנגנון העברת קבצים מאובטח (כגון כספות). מידע רגיש יאוחסן בצורה מאובטחת.

5.6. בכדי לתת מענה לאיומים הנובעים מחולשות אפשריות בשרשרת האספקה, על המשרד להיערך ארגונית מבחינת מדיניות, אחריות ההנהלה וניהול מחזור חיי ההתקשרות.

5.7. כמו כן, יש לבצע מיפוי ודירוג של הספקים על מנת להעריך את הסיכונים הכרוכים בהתקשרות עמו. המשרד יעמוד בקשר ישיר מול הספק, יתדרך אותו ויעגן בהסכם ההתקשרות את הבקרות הרלוונטיות לפעילות המתבצעת עמו בהתאם למתודולוגיה ומודל הביצוע של מערך הסייבר הלאומי.

6. <u>תחום הענן</u>

ספקים נותני שירות בתחום הענן יידרשו לעמוד בדגשים המופיעים בהנחיית יה"ב מס' 5.5 בנושא אבטחת מידע למעבר לענן ציבורי.

המשרד יציג את הפתרון בפני וועדת ענן ממשלתית.

7. <u>פיתוח מאובטח</u>

ספקים נותני שירות בתחום הפיתוח המאובטח יידרשו לעמוד בדגשים המופיעים בהנחיה מס' 5.13 בנושא פיתוח מאובטח.

8. <u>גישה מרחוק</u>

במידה ובמסגרת ההתקשרות עולה הצורך לחיבור הספק לתשתיות המשרד מרחוק, נקבעו כללים אשר על המשרד לעמוד בהם המשליכים גם על הספק.

9. <u>המענה</u>

מערך הסייבר הלאומי פיתח 3 תוצרים בהקשר זה על מנת לייצר סטנדרט אחיד לבדיקת ספק בהיבטי הגנת סייבר:

9.1. מתודולוגיה סדורה ל**שאלון ספקים**[i], המונה כ-90 בקרות, המחולקות ל-4 תחומי בדיקה: גישה מרחוק, דרישות רוחביות, אחסון בענן ופיתוח תוכנה מאובטח.

9.2. **מערכת יוב"ל**[ii] נועדה לתת מענה מקוון לבקרות אלו בכדי להקל על המשרדים לבצע התקשרות נכונה עם **ספקים מהותיים**[iii] ואחרים.

9.3. **בודקים** אשר סיימו בהצלחה הכשרה ייעודית ומבחן התמצות באופן בדיקת הספק ותהליך הסמכתו מול גוף התעדה ייעודי.

10. מועדים

נושא	תאריך	הערות
תקופת ההיערכות	31.12.2020	פרק הזמן הניתן למשרד לצורך התקשרות עם ספק שלא באמצעות תהליך הכשרה והתעדה של ספקים מהותיים המתבצע על ידי פירמידת ההכשרה והסמכה של ספקים.
מיפוי ודירוג ספקים	31.12.19	על המשרד לבצע מיפוי של הספקים איתם הוא מתקשר
התקשרות עם ספק בתקופת ההיערכות	31.12.2020	במידה והמשרד מעוניין לבצע התקשרות עם ספק מהותי אשר טרם ביצע את תהליך ההתעדה, יוכל המשרד לבצע את התהליך הנדרש מספק שדורג ברמה (B מילוי שאלון ספקים והוספת ראיות). *לאחר תאריך זה לא תותר התקשרות עם ספק מהותי ללא התעדה.

החרגה זו תתבצע עד לתאריך **31.12.2020 בלבד.**

***לאחר תאריך זה לא תותר התקשרות עם ספק מהותי ללא התעדה.**

[i] https://www.gov.il/BlobFolder/news/querysupply/he/%D7%A9%D7%90%D7%9C%D7%95%D7%9F%20%D7%A1%D7%A4%D7%A7%D7%99%D7%9D%20%D7%92%D7%A8%D7%A1%D7%94%201.1.xlsx

[ii] **מערכת יוב"ל** (יעדים ובקרות לארגון) - מערכת לניהול סיכוני סייבר ואבטחת מידע המהווה פלטפורמה לאומית אשר מורכבת ממספר רכיבים. בין רכיבי המערכת, קיים רכיב אשר מספק מענה לניהול סיכוני הסייבר של שרשרת האספקה בארגון/במשרד הממשלתי. המשרד רשאי לפנות לספק לצורך קבלת ממצאי דו"ח ההתעדה https://grc.cyber.gov.il/scripts/manage/login.aspx

[iii] **ספק מהותי / קריטי** –ספק המספק שירותים כגון: תמיכה ו/או תחזוקת מערכות מידע, אחסון נתונים רגישים מחוץ למשרד, שירותי מיקור חוץ טכנולוגיים או במקרה בו פגיעה בספק עלולה לגרום לנזק מהותי עבור המשרד