ממצאי סקר הסיכונים									המלצת יועץ המחשוב (עזרא)				הערות המועצה	אחראי	לו"ז לביצוע
#	ספרור תיעדוף	ממצא	תיאור	חומרה	סבירות	רמת איום	תיאור ההמלצה	מענה גוף מחשוב מועצה	פעולות לתיקון הליקוי	אומדן תקציבי לביצוע פעולות תיקון הליקוי					
1	7	**תיעוד איישור רשמי לרישום מאגרי המידע של המועצה, ותיערר תהליך אישור לרישום מאגרי המידע**	מאגרי המידע של המועצה הינם רשומים כחוק, והמועצה אינה מחזיקה ברישום רשמי.	4	4	רמת איום: 16 תקנות הגנת הפרטיות החדשות מחייבות רישום של מאגרי המידע, ומטילות סנקציות על גורמים אשר אינם עומדים בתנאי. כמו כן, המועצה חשופה בפני תביעות משפטיות בנוגע לרישום מאגר מידע ציבורי כנדרש בחוק.	ממלץ להנחות את היועץ המשפטי של המועצה לבצע בדיקה באשר לחובת המועצה לרישום מאגרי המידע שברשותה, ולעמוד בדרישות החוק.	בבדיקה מול ענת	החתמת הגורמים המתאימים במועצה. רישום המאגרים על ידי היועמש ברשם המאגרים במשרד המשפטים.	_____		בחתימות- טרם טופל	עזרא	01/12/2021
2	6	**אי ביצוע סקר סיכונים מהיבטי אבטחה פיסיים**	לא בוצע סקר סיכונים מהיבטי אבטחה פיסיים בשנים האחרונות.	4	4	רמת איום: 16 אבטחת מידע פיסית הינה נתבך חשוב במדיניות אבטחה מיטבית וכוללת. במידה ולא בוצעו הערכות בנוגע לרמת אבטחת המידע הפיסית, המועצה עלולה לסבול מאירועי דלף מידע וגניבות.	ממלץ לבצע סקר סיכוני אבטחת מידע מהיבט פיסי, אותו יוביל ממחה לאבטחה פיסית ובליווי מלא של מנהל הבטחון של התאגיד מנהל אבטחת המידע במועצה ישולב בתהליך בכפוף לרלוונטיות הממצאים.	הכנת סקר סיכונים	יועבר מפרט מיגון קיים על משרדי המועצה מקבט המועצה ויוטמע כחלק מתיק אבטחת מידע	_____		נדרש סקר סיכונים- הלייל הצעות היבטים פיזיים	עזרא	במיידי מרגע אישור
3	1	**תשתית הרשת האלחוטית (wifi) המיועדת לאורחים, מחוברת דרך ליבת המועצה**	חיבור האינטרנט האלחוטי (wifi) המיועד לאורחי המועצה, מחובר דרך ה FW המרכזי ויוצר חיבור בין רשת אינטרנט בלתי מוגנת ומוגבלת אל רשת הארגון הרגישה	4	4	רמת איום:16 החיבור הנ"ל עלול לאפשר לתוקף להשיג אחיזה בסביבת הרשת הארגונית, ותוך השקעת משאבים בינונית-נמוכה.	ממלץ להפריד לחלוטין את רשת האורחים מרשת הארגון.		לבצע סיגמנטציה-	_____		בוצע		
4	1	**הזדהות אל הרשת הארגונית המרכזיים מתאפשרת מכל עמדה כרשת ובאמצעות שם משתמש וסיסמה חלשות - בינוניות**	הזדהות אל שרתי הליבה של המועצה מבוצעת באמצעות שם משתמש וסיסמה חלשות- בינוניות, ולא רכיב OTP, ומכל עמדה בארגון. מעבר לכניסה דרך 2FA בלבד (המשתמש מקבל קוד מתחלף כל 5 דקות המותקן כאפליקציה בסלולארי) כך שקיימת ודאות כי המשתמש הוא זה שנכנס למערכת	4	3	רמת איום:12 בהיעדר מנגנון OTP, שרתי המועצה חשופים במידה רבה להתחברויות גורמים בלתי מורשים.	יש להטמיע פתרון הזדהות חזקה לסביבת הניהול כמתואר בתרשים ב', וכן למנוע את יכולת ההתחברות של כל עמדות הרשת, שאינן מיועדות לכך. -		רכישת FortiTokenMobile בכמות המשתמשים הנדרשת. מחיקת ומניעת משתמשים שאינם פעילים (רק מי שצריך להיכנס מרחוק מקבל גישה). כמות נדרשת: 50 רישיונות	כ230 ₪ למשתמש לכ שנה. כ11,500 ₪ סה"כ עבור 50 רישיונות		בוצע- לפני כחודש בוצע עדכון רשיונות VPN עם הזדהות TFA		
5	1	**חוקת ה- FW הקיימת - אינה קיימת ומתעדת כראוי את התעבורה העוברת**	באופן כללי, ניתן לומר כי חוקת ה- FW חסרה. היא אינה מגבילה אוכפות בפועל הגבלות נחוצות, ומתעדת בצורה מיטבית את תעבורת התקשורת בין תחומים ברשת, לרבות היציאה ל- wan וחיבורים עם ספקים חיצוניים.	4	4	רמת איום : 16 בשל כך שהגדרות ה- FW הנוכחיות אינן מידע ארגונית מעודכנת המתאימה לאיומים (בפרט חוקים 2-13, 17,18, 21,24, 25, 30, 31, 35, 40,36, 45,50, 56, 60-62), ולהסיר אובייקטים ישנים.- הספקת והתקנת Firewall בכל אתר דרכו תועבר כל הרשת הארגונית. ניהול policy אחיד בין כל ה Firewall	ממלץ לעצב מחדש את חוקת ה- FW כולה ע"פ מדיניות אבטחת מידע ארגונית מעודכנת המתאימה לאיומים (בפרט חוקים 2-13, 17,18, 21,24, 25, 30, 31, 35, 40,36, 45,50, 56, 60-62), ולהסיר אובייקטים ישנים.- הספקת והתקנת Firewall בכל אתר דרכו תועבר כל הרשת הארגונית. ניהול policy אחיד בין כל ה Firewall	המלצה לרכוש פורטייגיט 100F- להתקין במועצה להטמיע את השרת דואר ברשת נפרדת בכתובת אחרת ולבצע הפרדה ברמת FW בין הרשת של השרת דואר לרשת הארגונית	בניין המועצה: FortiGate-101F Hardware plus 3 Year 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP) (FG-101F-BDL-950-36) אתרי קצה משניים: FortiGate-60F Hardware plus 3 Year 24x7 FortiCare and FortiGuard Unified Protection (FG-60F-(UTM) (BDL-950-36	דולר 9000 תלוי רישוי לפורטייגיט 101 פורטייגיט 60- תלוי רישוי- 8000 -₪ כ37,000 ש"ח	לא קיים FW - עזרא יטמיע קובץ לבדיקת המערכת, לאחר השלמת התקנת מערכת סייבר 2	עזרא	
6	1	**שימוש בהזדהות חלשת בהתחברות מרחוק**	בעת התחברות מרחוק, נדרש המשתמש להזין שם משתמש וסיסמא, ועל-כן המערכת עלולה להיות חשופה לגניבת סיסמאות, פריצת סיסמאות, וכיוצ"ב.	4	4	רמת איום: 16 פריצת סיסמא של משתמש תאפשר לתוקף להתחבר לכלל משאבי הארגון ללא ידיעת גורמי אבטחת המידע והמחשוב של המועצה	ממלץ להשתמש במנגנון • זיהוי חזק בעת התחברות מרחוק, המבוסס על כרטיס חכם/תעודהTOKEN דיגיטאלית/ וכיו"ב • יש Tokens להגדיר גוהל מוסדר במקרה של אובדן/גניבה		רכישת אימות דו שלבי להתחברות מרחוק- Fortigate OTP- פורטי תוקן	_____		בוצע		
7	1	גישה של מחשבים וציוד זר לרשת הארגונית ללא יכולת זיהוי ומניעה	התחברות פיזית לרשת הארגונית באמצעות התקן / מחשב זר ופריצת הרשת	4	3	רמת איום: 12 קביעת הסיסמאות ו/או חלוקת ההרשאות נעשתה עד היום באופן כזה שיוצר פערים מהיבטי אבטחת המידע.	רישוי NAC ארגוני		רכישת NAC ארגוני המאפשרת ביצוע monitoring ארגוני. (אפיון של מוצרים מובילים ייערך עתידית)-	רכישה חד פעמית מסוג פורטייגט		בוצע- באמצעות פיילוט תוכנת סייבר 2		06/10/2021
8	2	חדירת קבצים נגועים תוך מעקף רשת ארגונית / הגנות ואבטחת מידע	התקנת נזקה המספקת גישה חופשית לכל הרשת והוצאת מידע, השחתת מידע, הצפנת קבצים ומחיקת מידע ארגונ	3	4	רמת איום: 12 סיסמאות בעלות "מורכבות" נמוכה ניתנות לפריצה בקלות יתר בין אם מדובר בתוקף חיצוני או עבריין פנימי.	עמדות הלבנה להכנסת קבצים זרים לרשת הארגונית חסימת הורדת קבצים מ GMAIL, רשתות חברתיות, WhatsApp וכו'		רכש עמדות הלבנה חסימת שירותים אלו ב Firewall. חסימת התקני אחסון נתיקים (DOK) . הדרכות מודעות עובדים הורדת פריבילגיות משתמשים לרמת user בלבד וחסימת ADMIN מקומי.	כ- 41,000 אלף ₪		בוצע- לא נדרש קיימת תוכנת סייבר 2		

9		**היעדר בידול ממשקי הניהול ועמדות העבודה השוטפות**	לא קיימת הפרדה בין ממשקי הניהול לתחנות העבודה השוטפות, וכן ניתן לגשת אליהם מכל נקודה ברשת.	3	3	רמת איום: 9 תוקף ע"פ רוב מנסה להשיג אחיזה באחת מעמדות הניהול אשר מאפשרת לו שליטה והתפשטות מהירה ברשת, שימוש בעמדה מנהלתית לניהול ותחזוקה מקל על התוקף להשיג מטרה זו	יש להפריד את סביבת הסיסטם/אבטחת המידע המשמשת לניהול ציוד התקשורת, מערכות אבטחת המידע והשרתים, משאר סביבות הרשת באמצעות חוקת FW משופרת, וניהול גישה בממשקים עצמם.		יישום הדרישה מול ספק המחשוב של המועצה	-	נדרש לבצע האם הבידול מיושם בתוכנת סייבר 2.	עזרא	31-אוק
10	1	כניסת תוקף לרשת הארגונית מאפשרת לו לגשת לכל משאבי הרשת, המשתמשים והשרתים ללא מגבלות (רשת שטוחה)	פריצה דרך מחשב קצה מאפשרת גישה חופשית לכל הרשת והוצאת מידע, השחתת מידע ומחיקת מידע ארגוני	3	0	רמת חאיום: 12 שיטת החדירה לרשתות והתפשטות השכיחה ביותר הינה השימוש בהתקני DOK שאינם בדוקים ומאושרים ע"י עובדים בין אם בשוגג או במודע	סגמנטציה של הרשת למספר רב של רשתות משנה / אזורים (Zones) מתחומים ב VLAN נפרדים ומנוהלים ב Policy נפרד לכל Zone (מעבר שירותים נדרשים בלבד בין אזור לאזור.		רכש מתגים מנוהלים המספקים גם יכולות אבטחת מידע מסוג FortiSwitch הציוד הנדרש: 8 יחידות מתגי תקשורת מסוג (עבור משרדי המועצה): - FortiSwitch-148E-POE managed POE switch with 48GE +4SFP, 24 ports POE -with max 370W POE (FS 148E-POE) לרבות שירות למתג: FortiSwitch-148E-POE 1 Year 24x7 FortiCare -Contract (FC-10-S148P-247 02-12) 10 יחידות מתגי תקשורת מסוג (עבור בניני המועצה ואתרי הקצה): - FortiSwitch-124E-POE managed POE switch with 24GE +4SFP, 12 ports POE -with max 185W POE (FS 124E-POE) לרבות שירות למתג: FortiSwitch-124E-POE 1 Year 24x7 FortiCare -Contract (FC-10-S248P-247 02-12)	ש"ח 3500 E- 148 ש"ח 2100 E- 124 סהכ כ- 21,600 כולל עבודות סגמנטציה	נדרש לבצע האם הבידול מיושם בתוכנת סייבר 2 מייתר את הדרישה לסגמנטציה ברשת.	עזרא	31\10
11	3	**היעדר הצפנה של כלל תחנות הקצה כולל תחנות נייחות**	תחנות קצה נייחות והתקנים ניידים אינם מוצפנים.	3	3	רמת האיום: 9 דיסק קשיח שיאבד ו/או ייזרק בטעות ללא מחיקה / השמדה יכול להכיל מידע רב ולהגיע לגורם זר מחוץ למועצה	מומלץ להצפין את כלל תחנות הקצה - הן הנייחות והן הניידות, לרבות טלפונים סלולאריים וטאבלטים. ניתן לתעדף את סדר הפעילות בצורה הבאה: 1. טלפונים סלולאריים וטאבלטים (באמצעות ESET) 2. מחשבים ניידים (באמצעות Bit-Locker). 3 עמדות נייחות (באמצעות מערכת ייעודית ו/או - Bit Locker)		יישום הדרגתי של הדרישה מול ספק המחשוב של המועצה	-	נדרש לבצע האם הבידול מיושם בתוכנת סייבר 2 מייתר את הדרישה לסגמנטציה ברשת.	עזרא	31//0
12	4	חדירה דרך תחנת עבודה / מחשב נייד לרשת הארגונית באמצעות התקנת P2P Tunnel או העברת ransomware script או סקריפט VPN או העלאת פריבילגיות משתמש לרמת Administrator	פריצה דרך מחשב קצה מאפשרת גישה חופשית לכל הרשת והוצאת מידע, השחתת מידע, הצפנת קבצים ומחיקת מידע ארגוני	4	4	רמת איום: 16 חיבורי התקני זיכרון ניידים חושפים את המועצה לפוגענים ולדלף מידע.	התקנת EDR ארגוני על כלל תחנות הקצה והשרתים הכולל ניטור ומניעת הנזקות המתוארות לרבות תחנת קצה ההופכת לזומבי		רכישת רישוי EDR של ESET שהינו השלמה לאנטי וירוס (endpoint security) הארגוני. הרישוי הנדרש: ESET Dynamic Endpoint Protection עבור 150 משתמשים (הרישוי המומלץ הוא	רישוי והטמעה ₪ 30,000	נדרש לבצע האם הבידול מיושם בתוכנת סייבר 2 מייתר את הדרישה לסגמנטציה ברשת.	עזרא	01-מרץ
13			הקשחת גישה למחשבים רגישים במועצה	4	4		ממליץ		רכישת מערכת לקריאות אצבע	בדיקת מחיר	ממתינים להצעה מקומיין - על מערכת קורא טביעת אצבע במקום כרטיסים	עזרא/רונן	01-מרץ
14	5	היעדר ניטור אירועי סייבר	המועצה מקבלת שירותי ניטור מחברת twistech, אך עיקר מאמצם מתרכז בניטור הרציפות התפקודית ולהיבטי מחשוב, ופחות לניטור אירועי אבטחת מידע. בפועל, למועצה לא קיים מוקד SOC מאויש וגורמי המקצוע במועצה לא מודעים לאירועי סייבר המתרחשים בה, לא בזמן אמת ולעיתים אף לעולם.	3	4	רמת תאיום: 12 במקרה של אירוע סייבר קריטי במועצה עלול להיגרם נזק רב בהעדר גורם מקצועי שיוכל לטפל באירוע באופן מידי. כמו כן, הסיכוי לניטור וגילוי תקיפה שאינה "רועשת" הינו נמוך מאוד.	מומלץ לשקול אפשרות קבלת שירותי ניטור מנוהלים מרחוק. (Managed SOC)		אפשרות והקמה של מערכת SIEM ללא SOK, ממולץ לשקול שירות SOK חיצוני כולל ניטור והתראות בזמן אמת,	כ- 90 אלף ₪ בשנה לכ-200 התקנים- מערכת SIM ללא SOK	נדרש לבדוק האם הניטור מיושם בתוכנת סייבר 2 מייתר את הדרישה לשירותים חיצוניים	עזרא	01-מרץ

13	4	**היעדר אכיפה רשתית לשימוש בתיבות דוא"ל אירגוניות בלבד- לא קיימת הגנה על הרשת הארגונית בבניין המועצה וביחידות השונות**	ברמה רשתית, לא מבוצעת אכיפה המונעת מגורמים שאינם מורשים להתחבר אל כתובות דוא"ל שאינן אירגוניות, כולל במחלקות רגישות במיוחד כמו המחלקה הפסיכולוגית.	3	4	רמת האיום: 12 פוטנציאל הנזק הטמון בדליפת מידע רגיש וחסוי הוא גדול מאוד מבחינה משפטית ותודעתית.	מומלץ לרכוש שירות צד שלישי בסינון דואר כולל יכולות DLP ו SENDBOX		רכישת רישוי: Microsoft 365 Business Basic בתוספת רישוי: office 365 Advanced Threat Protection לכמות של 150 משתמשים. (מומלץ למחוק משתמשים שאינם פעילים)	עבור DLP ו SENBOXS כ- 30 ₪ לתיבה לחודש- 4500 ₪ לחודש ל150 משתמשם- 54,000 ₪ לשנה עבור תיבת דולר ל365- 20 ₪ לתיבה- 3000 לחודש-150 משתמשים- 36,000 שח לשנה. +תהליך ניגרציה בהיקף ל150 שעות תלוי מערכת- 30-10 אלף ₪	עזרא- יבנה ארכיטקטורה והערכת מחיר/משתמשים ברשת	עזרא	01/03/2022

סה"כ