תשתיות מידע וטכנולוגיות בע"מ

תשתיות מידע וטכנולוגיות
יועצים לטכנולוגיית המידע ותשתיות הנדסיות

| משרד: 072-250.4385 | פקס: 072-250.7025 | נייד: 052-6704546 |

| ח.פ. 51377466-1 | ת.ד. 53035 ת"א | מיקוד 61530 | ezradyn@iti-il.com | www.iti-il.com |

21/01/2021

לכבוד
גב' ענת מור – מנכ"לית המועצה
מר רונן בגים – מנמ"ר המועצה
מועצה אזורית הגלבוע

הנדון: תוכנית עבודה מומלצת לרכש ציוד ורישוי לשיפור רמת אבטחת המידע הארגונית

שלום רב,

בהמשך ללימוד המצב הקיים וטופולוגית רשתות המחשוב במועצה האזורית גלבוע, אנו מציעים כיועצי אבטחת מידע ,לבנות תוכנית עבודה לשיפור רמת אבטחת המידע הארגונית שתכליתה כדלקמן. תוכנית העבודה נבנתה הן עבור המועצה (בניין המועצה ומשרדים מרוחקים) והן עבור החברה הכלכלית, קולחי גלבוע וגופי הסמך.

מטרות התוכנית:

א. הגברת רמת אבטחת המידע של הארגון והקטנת הסיכוי להצלחה במתקפת סייבר על המועצה.

ב. מניעת חשיפה של מאגרי המידע והמידע הרגיש במועצה לתוקפים חיצוניים.

ג. הרחקת תוקפים פוטנציאלים מהרשת הארגונית (IT) וממאגרי המידע של המועצה.

רכיבי הפתרון:

#	בעיה	משמעויות	פתרון	המלצה אופרטיבית
1	לא קיימת הגנה על הרשת הארגונית בבניין המועצה וביחידות השונות	חדירה לרשת הארגונית וגניבת, השחתת, מחיקת המידע הארגוני	הספקת והתקנת Firewall בכל אתר דרכו תועבר כל הרשת הארגונית. ניהול policy אחיד בין כל ה Firewall	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 (UTM) Protection (FG-60F-BDL-950-36)

| משרד: 072-250.4385 | פקס: 072-250.7025 | נייד: 052-6704546 |
| ח.פ. 51377466-1 | ת.ד. 53035 ת"א | מיקוד 61530 | ezradyn@iti-il.com | www.iti-il.com |

#	בעיה	משמעויות	פתרון	המלצה אופרטיבית
2	גישה דרך שרת הדואר לרשת הארגונית (כאשר שרת הדואר פועל מאותו סגמנט בו פועלת הרשת הארגונית)	חדירה לרשת הארגונית וגניבת, השחתת, מחיקת המידע הארגוני	מעבר לרישוי Microsoft 365	רכישת רישוי: Microsoft 365 Business Basicבתוספת רישוי: office 365 Advanced Threat Protection לכמות של 150 משתמשים. (מומלץ למחוק משתמשים שאינם פעילים)
3	גישה מאובטחת מרחוק (SSLVPN) באמצעות שם משתמש וסיסמה מספקת יכולות פריצה של הסיסמה וגישת תוקף חיצוני.	חדירה לרשת הארגונית וגניבת, השחתת, מחיקת המידע הארגוני	מעבר לכניסה דרך 2FA בלבד (המשתמש מקבל קוד מתחלף כל 5 דקות המותקן כאפליקציה בסלולארי) כך שקיימת ודאות כי המשתמש הוא זה שנכנס למערכת	רכישת FortiTokenMobile בכמות המשתמשים הנדרשת. מחיקת ומניעת משתמשים שאינם פעילים (רק מי שצריך להיכנס מרחוק מקבל גישה). כמות נדרשת: 50 רישיונות
4	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.	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)

| משרד: 072-250.4385 | פקס: 072-250.7025 | נייד: 052-6704546 |
| ח.פ. 51377466-1 | ת.ד. 53035 ת"א | מיקוד 61530 | ezradyn@iti-il.com | www.iti-il.com |

#	בעיה	משמעויות	פתרון	המלצה אופרטיבית
				10 יחידות מתגי תקשורת מסוג (עבור בנייני 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) **עבודות:** ביצוע עבודות סגמנטציה ברשתות המחשוב של התאגיד. (שיטת העבודה מפורטת למטה)
5	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.	התקנת EDR ארגוני על כלל תחנות הקצה והשרתים הכולל ניטור ומניעת הנוזקות 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 ל 3 שנים)
6	גישה של מחשבים וציוד זר לרשת הארגונית ללא יכולת זיהוי ומניעה	התחברות פיזית לרשת הארגונית באמצעות התקן / מחשב זר ופריצת הרשת	רישוי NAC ארגוני	רכישת NAC ארגוני המאפשרת ביצוע monitoring ארגוני. (אפיון של מוצרים מובילים ייערך עתידית)
7	חדירת קבצים נגועים תוך מעקף	התקנת נוזקה המספקת גישה חופשית לכל הרשת	עמדות הלבנה להכנסת קבצים	1. רכש עמדות הלבנה

| משרד: 072-250.4385 | פקס: 072-250.7025 | נייד: 052-6704546 |
| ח.פ. 51377466-1 | ת.ד. 53035 ת"א | מיקוד 61530 | ezradyn@iti-il.com | www.iti-il.com |

#	בעיה	משמעויות	פתרון	המלצה אופרטיבית
	רשת ארגונית / הגנות ואבטחת מידע	והוצאת מידע, השחתת מידע, הצפנת קבצים ומחיקת מידע ארגוני	זרים לרשת הארגונית חסימת הורדת קבצים מ GMAIL, רשתות חברתיות, WhatsApp וכו'	2. חסימת שירותים אלו ב Firewall. 3. חסימת התקני אחסון נתיקים (DOK) 4. הדרכות מודעות עובדים 5. הורדת פריבילגיות משתמשים לרמת user בלבד וחסימת ADMIN מקומי.

אומדן תקציבי (המועצה וכלל גופי הסמך):

רכש ציוד ורישוי המפורט במסמך זה: 270,000 ש"ח + מע"מ

עבודות: 150,000 ש"ח + מע"מ

אנו ממליצים לבצע רכש מסודר (יציאה להליך בקשה הצעות מחיר) על פי תוכנית העבודה המפורטת בטבלה לעיל.

בברכה,

עזרא דיין – יועץ

תשתיות מידע וטכנולוגיות בע"מ