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
מר רונן בגים – מנמ"ר
מועצה אזורית הגלבוע

הנדון: מוכנות המועצה לאירועי אבטחת מידע

שלום רב,

להלן מובאות המלצות ומסקנות להערכות לאירועי אבטחת מידע נוכח התגברות האיומים ושינויים באופי ההתקפות, ווקטור ושיטות תקיפה:

בעת האחרונה התרבו ההתקפות על ארגונים עסקיים ותשתיות עירוניות (חב' ביטוח שירביט, עיריית הרצליה, חב' עמיטל מערכות שילוח ולוגיסטיקה, עיריית ירושלים ועשרות ארגונים אחרים שלא הגיעו לכותרות ראשיות). קמפיין התקיפה השתכלל והופעל על החולשות הבאות:

א. גישה דרך חולשות שהתגלו במערכות מידע של ספקים חיצוניים – חדירה דרך מערכות מידע של הספק לרשת הלקוח
ב. שרת דוא"ל – חדירה לשרת דואר דרך פורטים פתוחים לתעבורת פרוטוקול דואר כדוגמת 443,587,993 ומשם לרשת הארגונית.
ג. הקמת VPN פרטי בין מחשב ברשת ארגונית לתוקף לאחר החדרת סקריפט או קובץ הפעלה ויצירת VPN tunneling בין הארגון לתוקף לגניבת מידע ולשיטוט ברשת הארגונית.
ד. אי ביצוע עדכוני אבטחה (software patch) שעודכנו על ידי יצרני התוכנות והציוד: למערכות הפעלה, מתגים וציוד רשת, עדכוני קושחה בציוד אבטחת המידע – בבחינת פרצה ממנה ניתן לגשת לתוך הרשת הארגונית.

המלצות ליישום מיידי

להלן המלצות לרכש ויישום מיידי:

א. מעבר תיבות דואר לשרת מיקרוסופט אופיס 365 – הרחקת התוקף מרשת התקשורת של הארגון. התוקף אינו יודע היכן נמצא הארגון. ההגנה בענן 365 גבוהה יותר. ההמלצה היא לרישוי ברמת אבטחה גבוהה (MFA).
ב. רכישת והקשחת Firewall במועצה והעברת כלל התעבורה הן מהחברה לאוטומציה והן רשתות Wi-Fi, טלפוניה ורשת ארגונית – דרכו בלבד.

| 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 |

ג. שדרוג האנטי וירוס ביחידות הקצה למערכת EDR המספקת מעטפת אבטחה גבוהה על יחידת הקצה מעבר לקיים היום (הגרסה הקיימת במחשבי המועצה אינה מספקת מעטפת הגנה כוללת, אינה מספקת הגנת וירוס כופר (ransomware) וניתן לשתול סקריפטים להפעלת VPN tunneling ללא ניטור של אנטי וירוס.

ד. מעבר לארכיטקטורת Zero Trust network וביצוע הפרדה וסגמנטציה של הרשת הארגונית באמצעות ניהול VLAN נפרדים ברמת מחלקה. נדרש רכש של מתגים Forti Switch סדרה 100 לניהול הרשת וסדרה 200 לניהול ה backbone (שדרת תקשורת מרכזית), המאפשרים ניהול סגמנטים ורשתות VLAN וניטור על ידי ה Firewall ברמת פורט בודד.

ה. ניטור אירועים ברשת הארגונית באמצעות מערכת NAC לניטור כלל יחידות הקצה, חיבורים זרים לרשת, תעבורת מידע החוצה לשרתים חיצוניים (ניטור P2P tunneling), ניטור שינויים ב firmware במתגים וציוד רשת ומניעת גישה ברמת זיהוי התקנים ברשתות המחשוב.

יישום המלצות אלו בדחיפות הינו קריטי למוכנות המועצה למתקפות סייבר.

בברכה,

עזרא דיין – יועץ
תשתיות מידע וטכנולוגיות בע"מ