תשתיות מידע וטכנולוגיות
יועצים לטכנולוגיית המידע ותשתיות הנדסיות

תשתיות מידע וטכנולוגיות בע"מ
| משרד : 072-250.4385 | פקס : 072-250.7025 | נייד : 052-670.4546 |
| ח.פ. 51377466-1 | משה לוי 14, ראשון לציון | ezradyn@gmail.com | www.iti-il.com |

11/01/2021

לכבוד:

רונן בגים-מנהל מערכות מידע
מועצה אזורית הגלבוע

העתק:
ענת מור- מנכ"לית מועצה

הנחיות -דרישות סגמנטציה של רשתות התקשורת

ביצוע סגמנטציה של רשתות התקשורת ומעבר מרשת class c הקיימת למספר רשתות משנה (VLAN) המגדירות טווחי כתובות מתוחמים ביניהן (בסגמנטים קטנים מ 254 כתובות כדוגמת 4,8,16,32 כתובות בכל VLAN), המנוהלים על ידי Firewall מרכזי וחסומות אחת מהשנייה פרט לפורטים ושירותים נדרשים לתעבורה בין אזורים (zones) / רשת משנה לרשת משנה (להלן מדיניות policy) וזאת על פי ארכיטקטורת zero trust network architecture . יידרש ליישם, להגדיר את כלל הכלים כדוגמת FW, IPS, WAF, EDR לטובת הקשחת רשתות התקשורת של המועצה.

יעדים:

(א) הגברת רמת אבטחת המידע הארגונית ברמת הפרדה מחלקתית בין רשתות המשנה ומניעת זליגה / פריצה של כלל הרשת במידה ונפרצה יחידת קצה במחי מסוימת.

(ב) הגברת יעילות ומהירות תעבורת הרשת הארגונית – הקלת צווארי בקבוק ומיתוג מהיר בין יחידות קצה.

תשתיות מידע וטכנולוגיות בע"מ
| משרד : 072-250.4385 | פקס : 072-250.7025 | נייד : 052-670.4546 |
| ח.פ. 51377466-1 | משה לוי 14, ראשון לציון | ezradyn@gmail.com | www.iti-il.com |

(ג) הפרדת שירותים העלולים להיות יעד לפריצה : רשתות Wi-Fi, טלפוניה, מדפסות וכו' והרחקתן מרשת המחשבים ומרשת השרתים (מכונות VM, רשת ניהול שרתים) של המועצה.

(ד) הפרדת יחידות חיצוניות אקסטרניות ומשתמשים בחיבור מרחוק, מרשתות הארגוניות והנגשת שירותים מוגדרים בלבד לאותן יחידות.

(ה) תיחום ברמת DMZ מופרד של שרתים ושירותים המופנים לאינטרנט ומהווים מקור פוטנציאלי להתקפות כדוגמת שרתי אפליקציות ו- WEB, מחשבים ניידים, מחשבים בחדר ישיבות, ומחשבי קצה הפועלות מול רשתות חברתיות.

ביצוע הסגמנטציה יכלול:

(א) שדרוג כלל ציוד אבטחת המידע הקיים (Firewall) לגרסת יצרן האחרונה.

(ב) החלפת המתגים הקיימים במתגים תוצרת Fortinet בכל מבני המועצה.

(ג) חלוקת הרשת הארגונית למספר רשתות משנה (VLAN) אשר יוגדרו ברמת היישום, כמפורט בטבלה להלן (Zones). לכל אזור תוגדר מדיניות (policy) נפרדת ב Firewall הכוללת שירותים מותרים ופורטים (לרבות כיווניות) המועברים בינו לבין אזורים אחרים :

Zone	תיאור	מדיניות (policy)
110	רשת ניהול שרתים ואמצעי אחסון	MGMT
120	סביבת שרתים פנימיים : DC ראשי ומשני, DB, File Server מקומי ושרתים המספקים שירותים מקומיים בלבד.	מדיניות שרתים פנימית
130	סביבת DMZ משתמשים בחיבורים מרוחקים (SSLVPN), שרת RDS + שרת DC הקורא את המידע בתעבורה חד כיוונית מ DC ראשי.	RDS
140	סביבת רשת מדפסות ושרת תורי הדפסה	הדפסות
150	סביבת רשת טלפוניה, מערכת ניהול מוקד ו PBX טלפוניה	טלפוניה
160	רשת בקרת מתקנים(OT)	OT

תשתיות מידע וטכנולוגיות בע"מ
| משרד : 072-250.4385 | פקס : 072-250.7025 | נייד : 052-670.4546 |
| ח.פ. 51377466-1 | משה לוי 14, ראשון לציון | ezradyn@gmail.com | www.iti-il.com |

Zone	תיאור	מדיניות (policy)
200	משתמשים מנכ"ל מועצה	Users
205	משתמשים מחלקת חינוך	Users
210	משתמשים מנהל שירות לתושב	Users
215	משתמשים מנהל פיתוח	Users
220	משתמשים מחלקת מרכזים קהילתיים	Users
225	משתמשים מועצה מקומית	Users
230	מחלקת שירותים חברתיים	Users
235	משתמשים לשכת ראש המועצה	Users
240	משתמשים מחלקת פיקוח ורישוי עסקים	Users
245	משתמשים מחלקת הנדסה	Users
250	משתמשים מחלקת גזברות	Users
255	משתמשים מחלקת תרבות	Users
260	משתמשים מחלקת גביה	Users
265	משתמשים בטחון	Users
270	משתמשים יחידות הרכש	Users
275	משתמשים -תכל'ס- מרכז צעירים בגלבוע	Users
280	משתמשים יחידה סביבתית ומחלקת פיקוח	Users
285	משתמשים החברה הכלכלית הגלבוע	Users
290	משתמשים דורות בגלבוע(עמותה)	Users
295	משתמשי VPN בחיבור מרחוק	Users
300	חדרי ישיבות	DMZ
400	רשתות חברות עירוניות	EXWAN
410	רשת תאגיד קולחי הגלבוע	EXWAN
420	רשת Wi-Fi פנימית מועצה	WIFI
430	רשת Wi-Fi אורחים מועצה	WIFI
440	רשת מצלמות	CCTV
450	רשת שעוני נוכחות	SYN

תשתיות מידע וטכנולוגיות
יועצים לטכנולוגיית המידע ותשתיות הנדסיות

תשתיות מידע וטכנולוגיות בע"מ
| משרד : 072-250.4385 | פקס : 072-250.7025 | נייד : 052-670.4546 |
| ח.פ. 51377466-1 | משה לוי 14, ראשון לציון | ezradyn@gmail.com | www.iti-il.com |

מטרה:

רשת תקשורת מנוהלת ומנוטרת ברמת הפורט הבודד

רשת התקשורת תנוהל ברמת הפורט הבודד ותכלול ניהול הן ברמת רשת התקשורת והן בהתאם לדרישות ה policy החל על הפורט הבודד. ניהול ברמת הפורט הבודד יאפשר זיהוי חיבורים זרים ברמת MAC Address וחסימת רכיבים, יחידות קצה ומחשבים לא מוכרים.

עזרא דיין

ממונה אבטחת מידע