



2 תשתיות טכנולוגיות ואיומים בעיר הדיגיטלית ערן טוך

ערן טוך, "תשתיות טכנולוגיות ואיומים בעיר הדיגיטלית", מתוך העיר בעידן הדיגיטלי: תכנון, טכנולוגיה, פרטיות ואי שוויון. עורכת שלי חתוקה, אוניברסיטת תל אביב, 2018, עמ' 40-53.

תשתיות טכנולוגיות ואיזמים בעיר הדיגיטלית

ערן טוך

כרגע אף רשות לא מונחת במטה הסייבר, זה אומר שיכולה להיות רשות אפילו בלי שום מנגנון אבטחת מידע, אפילו לא אנטי-וירוס. אין הנחיה, אף אחד לא מונחה ואף אחד לא בודק. בתור נציג המנמ"רים בכנסת הסברתי למטה הסייבר שברגע שתהיה בעיה, חדירה לאחת הרשויות, הבעיה תהיה ארצית, לא רשותית. יגנבו פה כספים וחדירה למערכות. עיריית ראשון לציון סולקת מיליארד וחצי שקל, צריך להבין שאלו מערכות מאוד מאוד כבדות. צריך לתת את הדעת על העניין הזה. רשות שהמנמ"ר שלה לא מספיק מבין באבטחת מידע, אין אבטחה.¹

התפתחויות טכנולוגיות שונות הנחו את התפתחות העיר מאז תחילת תהליך העיור. גורמים כגון ביצור, תחבורה ואנרגיה השפיעו על מיקום ועל מבנה העיר. בעשורים האחרונים טכנולוגיות המידע – מונח שעניינו שימוש בטכנולוגיות מחשוב ותקשורת לשם ניהול ועיבוד מידע – תופסות מקום הולך וגובר בערים. טכנולוגיות מידע מבוססות מחשוב התפתחו בהקשר ארגוני ותעשייתי במחצית השנייה של המאה העשרים. תחילה כללו טכנולוגיות המידע מחשבים שביצעו פעולות חישוב ואגירת נתונים, ובהמשך התפתחה טכנולוגיה מתקדמת יותר, שכללה רשתות מחשבים, שהתחברו לבסוף ברשת האינטרנט. מזעור המחשוב, התפתחות רשתות לתקשורת אלחוטית על גבי סרט רחב והתפתחויות טכנולוגיות לשמירה ולעיבוד מידע רחב היקף מאפשרים פריסה של טכנולוגיות שונות, שפעם היו מוגבלות לתפעול תעשייתי או לאזורים מוגדרים כגון שדות תעופה.² כיום עם הפיכת טכנולוגיות רבות לזולות ולפשוטות ערים רבות הופכות ל"ערים חכמות" באמצעות הטמעה ובנייה של תהליכי עבודה על גבי היישומים הטכנולוגיים.

הטמעה של טכנולוגיות בעיר מונעת מריבוי כוחות ואינטרסים. ערים מעוניינות לצמצם עלויות של אספקת שירותים עירוניים ולספק שירות טוב יותר; ספקי טכנולוגיה שהתמחו במגזר התעשייתי מעוניינים ליצור שווקים חדשים למוצריהם; כמו כן חברות פרטיות ואפילו אזרחים יוצרים סביבה טכנולוגית מבוססת מידע ושווקים, ההופכים את חוויית התושבות או הביקור בעיר למתוחכמת יותר. פרק זה מתמקד בטכנולוגיות המושמעות בערים ובאופן שיש להיערך לסיכונים המתלווים להן. לפרק זה ארבעה חלקים. החלק הראשון מציג את הטכנולוגיות העיקריות הקיימות היום בערים. החלק השני דן בתהליכים טכנולוגיים. החלק השלישי סוקר

¹ איציק כרמלי (מנמ"ר ומרכז תוכנית עיר חכמה, עיריית ראשון לציון), 8.9.2016.

² Antony Bryant et al., "Information Systems History: What is History? What is IS History? What IS History?... And Why even Bother with History?," *Journal of Information Technology* 28, no. 1 (2013): 1–17.

איזמים שונים על מערכות המידע של העיר בעידן הדיגיטלי. איזמים אלו כוללים התקפות על תשתיות טכנולוגיות בעיר (חומרה, תוכנה ויישומים) ועל מסדי נתונים. חלק זה כולל מיפוי של סוגים שונים של התקפות, והוא מאורגן באשר לסוג התשתית המותקפת ולסוגי ההתקפה. החלק הרביעי מוקדש להמלצות שונות להגנה על התשתיות הדיגיטליות ועל פרטיות התושבים בעיר.

השמעה של טכנולוגיות בעיר מונעת מאינטרסים רבים: ספקי טכנולוגיה המחפשים שווקים חדשים, חברות פרטיות ותושבים. פרק זה יתמקד בסיכונים המתלווים לכך.

טכנולוגיות עכשוויות בעיר כוללות מגוון רחב מאוד של מערכות. מגוון רחב זה מאורגן לפי שלושה ממדים עיקריים: שטח היישוב, הרמה הטכנולוגית והאסטרטגיה הארגונית של המערכת.

הטכנולוגיות בעיר הדיגיטלית מבוססות על מערכות המזרימות מידע דרך רשת תקשורת ועל מערכות לקבלת החלטות הפועלות על פי מידע זה. טכנולוגיות עכשוויות בעיר כוללות מגוון רחב מאוד של מערכות – החל ביישומים לחיסכון במים, דרך מערכות מידע לניהול מידע הנדסי ותכנוני וכלה ביישומונים לתושבים בטלפון החכם. כדי לנתח ולארגן מגוון רחב זה אנו מאמצים כמה שיטות קטלוג, המאורגנות לפי שלושה ממדים עיקריים: שטח היישוב, הרמה הטכנולוגית והאסטרטגיה הארגונית של המערכת.

• שטח היישוב

אפשר לארגן את הטכנולוגיות על פי שטח הפעילות שבו הן מיושמות, כגון אנרגיה, תחבורה, קשר עם התושב, מים, וכן הלאה. בטבלה 2.1 שלהלן, שנערכה על סמך הספרות האקדמית,³ מוצגות קטגוריות של מערכות טכנולוגיות הנפוצות בערים עכשוויות. הטבלה שלהלן מציגה את שטחי היישוב העיקריים, והיא מאורגנת על פי רמת ההטמעה הפיזית הנדרשת – משדות שבהם יש הטמעה פיזית ניכרת לשדות שבהם בדרך כלל יש צורך מופחת בהטמעה פיזית של השירות בתשתיות העיר (טבלה 2.1).

• הרמה הטכנולוגית

ממד זה מתאר את המקום ואת התפקיד של הטכנולוגיה הספציפית בתוך המארג של העיר, כך למשל אם מדובר בטכנולוגיה תשתיתית המותקנת בשטח או במערכות לניתוח מידע. קטגוריזציה זו מתארת לנו את המיקום של הטכנולוגיה ב"רשרת המזון" הטכנולוגית ואת האופן שבו פתרונות שונים משתלבים יחד,⁴ כפי שמתואר בטבלה 2.2.

טבלה 2.1: שטחי יישוב של טכנולוגיות דיגיטליות נפוצות בערים עכשוויות

| תחום | יישומים טכנולוגיים | דוגמאות |
|--------------------------------|---|---|
| תחבורה ותנועה | שיפור אמצעי תחבורה שונים והקטנת העלות שלהם. | יישומים לארגון תחבורה ציבורית, לארגון הסעות בין תושבים (ride sharing), לניהול משאבים כגון חנייה וכבישים וכו'. |
| רחובות ובניינים חכמים | העשרה של הסביבה הפיזית בטכנולוגיה במטרה להפוך אותה ליעילה, לאפקטיבית ולזולה יותר. | ניהול תאורת רחוב, עמדות תצוגה בעיר, מערכות לניהול בנייני מגורים. |
| סביבה, מים ופסולת | ייעול הטיפול במשאבים בסיסיים בעיר כגון מים וטיפול בפסולת – הן בחיסכון בהקצאת המשאבים הן בזיהוי של זיהומים ושל מפגעים ובטיפול בהם. | השקיה דיגיטלית, חלוקת מים, זיהוי נזילות ממערכות להובלת מים, טיפול במי קולחים, זיהוי זיהומים במים ובאדמה, זיהוי כמות הפסולת בפחים, ניהול של מערך פינוי פסולת, בקרה על זיהומים תעשייתיים. |
| אנרגיה | ייעול של מערכות ייצור, הולכת אנרגיה והשימוש בה וניהולן של מערכות אלו. | ניתוח ובקרה של רשתות חשמל, ייצור אנרגיית שמש ואחסונה, מערכות לניהול פאנלים סולריים במרקם העירוני, ניהול צריכת חשמל של צרכנים פרטיים ועסקיים. |
| טיפול במצבי חירום | שימוש בטכנולוגיה כדי לשפר ולהגיב טוב יותר למצבי חירום שונים. | מערכות לאיתור ולטיפול במצבי מצוקה, לניהול כוח אדם המגיב למצב ולזיהוי אוטומטי של רעידות אדמה, של שיטפונות, ושל מצבי חירום נוספים. |
| אבטחה ומעקב | מעקב ואבטחה של אזורים רחבים. | פריסה של מצלמות מעקב וחיישנים שונים, ניתוח אוטומטי של וידאו. |
| ממשק עם תושבים ובינם לבין עצמם | מערכות המאפשרות תקשורת ואינטראקציה בין הרשות לבין התושבים או בין התושבים לבין עצמם. | מערכות שונות כגון רשתות חברתיות עירוניות, שיתוף הציבור בתכנון עירוני, מעקב אחר פעולות תושבים ברשתות החברתיות. |

טבלה 2.2: מדרג הטכנולוגיות הנפוצות בערים

| רמה טכנולוגית | יישומים | דוגמאות |
|---------------|--|--|
| יישומים | מערכות הפונות לפתור בעיה או צורך בשטח יישוב מסוים. | יישום לזיהוי של מצב פחי האשפה או יישוב המיידע תושבים בנוגע לאירועים באזורם. |
| תשתית לוגית | תוכנה המאגדת מידע והמאפשרת הפעלה של מספר גדול של יישומים. | מערכות GIS (Geographical Information Systems) המאפשרות ניהול מידע גיאוגרפי שעל בסיסו נבנים יישומים. |
| תשתית פיזית | מערכת הפרוסה בשטח העיר והכוללת תוכנה וחומרה המאפשרות ליישומים ולתשתית לוגית יכולת להתקשר לשטח. | מערכות שכאלו כוללות רכיבי IoT (Internet of Things), שהם חיישנים ורכיבים פועלים המחוברים לרשת האינטרנט כגון מצלמות אבטחה, חיישנים כימיים, פנסי רחוב מקושרים וכו'. |
| רשתות תקשורת | רכיבי תוכנה וחומרה המקשרים בין אלמנטים שונים בעיר הדיגיטלית ובין השכבות השונות. | רשתות תקשורת בעיר הדיגיטלית כוללות מתגים, קווים אופטיים, קווי נחושת, אנטנות WiFi, רשתות 4G ו-5G סלולריות, רשתות Fog וארכיטקטורות תקשורת נוספות. |

3 Vito Albino, Umberto Berardi, and Rosa Maria Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives," *Journal of Urban Technology* 22, no. 1 (2015): 3–21
 של מסמך הערים החכמות של IBM: "A Vision of Smarter Cities," IBM Institute for Business Value, 2009, https://www-03.ibm.com/press/attachments/IBV_Smarter_Cities_-_Final.pdf; Paolo Neirotti et al., "Current Trends in Smart City Initiatives: Some Stylised Facts," *Cities* 38 (June 2014): 25–36, <https://doi.org/10.1016/j.cities.2013.12.010>
 4 W. M. da Silva et al., "Smart Cities Software Architectures: A Survey," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing* (March 2013), 1722–1727

לכל מדינה מאפיינים ייחודיים משלה. בישראל נפוצים במיוחד הפרויקטים להלן:

מערכות מידע לתושב – מערכות המספקות מידע לתושבים בצורה אקטיבית, כדוגמת מערכת דיגיטל בתל־אביב, כרטיס תושב באשדוד, או אפליקציה לתושב בחיפה. מערכות אלו מספקות מידע מותאם אישית בצורה אקטיבית (בעזרת מסרונים sms ומערכות נוספות), כך למשל על אירועים בתחומי העניין של בעלי הכרטיס או על בעיות ספציפיות באזור המגורים. המערכת משתמשת במאגר מידע, הכולל פרופילים של תושבים המתארים את תחומי העניין שלהם והמתאים מידע על אירועים לתושבים. בערים רבות יישומים אלו קשורים לכרטיס תושב המזהה את התושב בשירותים עירוניים או מסחריים. הדוגמה הבאה, מדברי יוסי בן סימון, מנמ"ר עיריית אשדוד, מתארת כיצד עיריית אשדוד מתכננת את מערכת המידע לתושב:

"בהקשר של כרטיס תושב? יהיה איסוף מידע לפי תחומי עניין, לפי גיל, לפי סוגי התרבות שאתה חושב שמראש יעניינו אותך. אתה יכול להתחיל לדחוף מידעים לתושבים ממש פר דברים שהם מתעניינים בהם ולא סתם להציף אותם במידע. כאשר אתה שולח להם מידע שמעניין אותם אתה מתחיל להגיע לתושב, התושב מתחיל לקבל ערך, שמתייחסים אליו באופן אישי. בעבר דיברו על כרטיס פלסטיק שלא יצא לפועל. עכשיו שאנחנו הולכים לעולם הדיגיטלי זה תפס תאוצה, ויותר קל לעשות את זה".⁵

מערכות תאורת רחוב מקושרת – מערכת תאורת רחוב שכוללת נורות לד (LED) חסכוניות וכן הטמעה של חיישנים שונים (כולל חיישני רעש, טמפרטורה, לחות וזיהום אוויר) ורכיבים נוספים (כגון רשתות WiFi). מערכת התאורה מחוברת בעזרת סיבים אופטיים ומשמשת תשתית לפריסה פיזית של רכיבי העיר הדיגיטלית. מערכות אלו הן יעילות, כיוון שהן מאפשרות חיטון ניכר בעלות הפריסה ובתפעול המערכות. כפי שיוסי בן סימון מתאר את היכולות של המערכת, מדובר ב"מערכות בקרת תאורה שמאפשרות להדליק את התאורה לפי זמני היום, להוסיף עוצמה של תאורה, להוריד עוצמה, הכול ביחס. נגיד בשתיים בלילה לא צריך את אותה עוצמת תאורה כמו בשמונה בערב, כי בשתיים בלילה בקושי יש תנועה. אז לא סתם מדליקים את כל הפנסים, מדליקים חלק או שמנמיכים את העוצמה".⁶

מערכות השקיה – למערכות השקיה המשלבות חיישני לחות, חיישני מזג אוויר, מערכות ניהול וטפטפות יש פוטנציאל להוריד את העלות הכוללת של ההשקיה ברחבי העיר. הפוטנציאל לחיטון במערכות שכאלו הוא גדול, כפי שמדווח אבי בן חמו, מנכ"ל עיריית נתניה:

"בתהליך שהתחלנו הכנסנו טכנולוגיות מיוחדות להשקיה, הצלחנו כבר בחלק הראשון לחסוך. אני אתן לכם ככה לסבר את האוזניים – אנחנו השקינו כחמש מאות דונם באמצעות כמעט שני מיליון קוב מים, ועכשיו אנחנו משקים כמעט פי שניים; גדלנו בשטחי הגינון, יכולנו לאפשר לעצמנו לגדול בשטחי הגינון במיליון ושלוש מאות אלף כתוצאה מהשינוי הזה".⁷

מערכות חיוב וגבייה – פיתוח מערכות לחיוב ולגבייה של תשלומים שונים, כולל ארנונה, דוחות שונים וחריגות בנייה. אחת המערכות הגדולות פותחה בעיריית תל־אביב, כפי שמדווח אסף זמיר, סגן ראש עיריית תל־אביב-יפו: "מחוג זה משהו שאף אחד לא התייחס אליו כחדשני, אבל הוא בטח קשור לעיר חכמה... מחוג זה מערכת חיוב וגבייה, שהעירייה בנתה יחד עם NESS ב־180 מיליון שקל כדי לוודא שכולם משלמים את הארנונה שלהם. [המערכת] בערך כיסתה את ההשקעה שלה בשנה וחודש".⁸

5 יוסי בן סימון (מנמ"ר, עיריית אשדוד), 25.9.2016.
6 שם.
7 אבי בן חמו (מנכ"ל עיריית נתניה), 8.8.2016.
8 אסף זמיר (סגן ראש עיריית תל־אביב), 7.8.2016.

מערכות אבטחה ומעקב – פרויקטים בתחום ה"עיר הבטוחה" או "עיר ללא אלימות", הכוללים מערכות מעקב שונות ובעיקר מצלמות אבטחה. בערים רבות ישנו שימוש במערכות המבצעות ניתוח אוטומטי של הוידאו המתקבל מן המצלמות והמאפשר לזהות אירועים כגון מעבר לאזור מסוים, התקבצות של כמה אנשים באזור או עצירה של מכוניות בשול הדרך. עיריות מטמיעות מערכות שכאלו בעיקר בגלל החיטון בכוח האדם במוקדי אבטחה, ובזכות היכולות רבות העוצמה לניתוח האירועים בעיר, כפי שמדווח יוסי בן סימון:

"בתחום הסייף סיטי [safe city] הקמנו פה מערכת מוקד רואה, ופרסנו כ־150 מצלמות נכון להיום. המצלמות האלה מחוברות למוקד העירוני עם מערכת שו"ב [שליטה ובקרה], וחלק מהמצלמות כבר משולבות בהן טכנולוגיות של וידאו אנליטית. הרי אי אפשר להושיב מוקדנים יום שלם על 150 מצלמות ולנסות לראות אירועים בזמן אמת. אז יש מקומות ששמים מצלמה חכמה, שידעת לבצע ניתוח אנליטי של אירוע ולהקפיץ את התמונה למוקדן הראשי".⁹

• האסטרטגיה הארגונית של המערכת

המונח אסטרטגיה ארגונית של המערכת מתייחס לגישה הארגונית ביחס לפתרון הטכנולוגי והאופן שבו הוא בנוי.¹⁰ טכנולוגיות שונות מופעלות בידי גורמים שונים, ולכל טכנולוגיה שכזו גישה ארגונית מסוימת המכתיבה היכן, מתי, ובאילו תנאים הטכנולוגיה יכולה לפעול. כך למשל, ישנן טכנולוגיות המופעלות בידי הרשות המקומית או הארצית (כגון מערכות מידע בתחנות אוטובוס), ישנן טכנולוגיות המופעלות בידי חברות פרטיות (כגון היישומון Moovit) וישנן אף טכנולוגיות המפותחות בידי התארגנויות של תושבים. **השימוש במושג "אסטרטגיה ארגונית" נועד לתאר את הקשר שבין היוזמה וההפעלה של המערכות לבין האופן שבו הן מיושמות במרקם העירוני.** טבלה 2.3 מתארת אופנים שונים שבהם פרויקטים טכנולוגיים יכולים להיות מיושמים.

טבלה 2.3: קטלוג של אסטרטגיות ארגוניות

| האסטרטגיה הארגונית | מאפיינים | דוגמאות |
|--------------------|--|--|
| גישת top-down | גישה זו מתמקדת בתכנון היררכי של המערכת, שבו העירייה (בדרך כלל) מתכננת את המערכת ומיישמת אותה באופן ריכוזי ותוך שימוש במשאבים העומדים לרשותה. | מערכות ניהול אשפה, ניהול תחבורה ציבורית. |
| גישת bottom-up | זו גישה לא־היררכית, שבה בניית המערכת היא בידי תושבים או התאגדויות מקומיות. פעמים רבות העירייה או הגוף השלטוני מספקים נתונים או משאבים מסוימים, והיישומים נבנים בידי התושבים. | רשתות חברתיות הפועלות בבניינים, יישומים המפותחים בידי התושבים, רחובות ואזורים אורבניים, יישומי "צבע אדום" המתחברים לממשק ההתראות של פיקוד העורף. |
| גישה מעורבת | אלו יישומים המפותחים בידי חברות פרטיות או ארגונים ומיושמים בעיר. | אפליקציות crowdsourcing כגון Moovit. |

9 יוסי בן סימון (מנמ"ר, עיריית אשדוד), 25.9.2016.
10 Neirotti et al., "Current Trends"

היישומים הטכנולוגיים הנפוצים בישראל: מערכת מידע לתושב, מערכות תאורת רחוב מקושרת, מערכות השקיה, מערכות חיוב וגבייה, מערכות בקרה ומעקב.

ב הקמה של מערכות טכנולוגיות בערים

בתהליך ההקמה של מערכות טכנולוגיות בערים ניתן לזהות שלושה תהליכים עיקריים.

• **אינטגרציה מרחיבה של המידע בעיר.** חלק ניכר מן הפרויקטים הדיגיטליים, בעיקר פרויקטים המתרכזים בבניית תשתית לוגית, מתמקדים באינטגרציה הולכת וגוברת של המידע בעיר. מטרת האינטגרציה היא להפוך תהליכים ליעילים יותר, ולאפשר שליטה גדולה יותר בנעשה בעיר. כפי שמנסח זאת יוסי בן סימון,

"כשאני אומר אינטגרציה הכוונה היא שיש היום מערכות שונות, אבל המערכות לא יודעות לדבר בינן לבין עצמן. לדוגמה, הלך פנס ברחוב מסוים, נשרף. עוד לפני שהתושב יתלונן, אם הייתה מערכת חכמה, היא הייתה מזהה ופותחת פנייה אוטומטית במערכת ה־ CRM. מערכת ה־ CRM אוטומטית תזהה שזה ממחלקת החשמל ותוציא הפנייה לטיפול של אגף החשמל, וככה התיקון מתבצע אוטומטית לפני שמישהו מרים טלפון".¹⁵

• **חיזוי התנהגות התושבים.** מערכות העיר הדיגיטלית מתפתחות מעבר לתגובה לפניית או לפעולות של המשתמשים, ומתמקדות בזיהוי התנהגות המשתמשים (בעיקר התושבים) והעדפותיהם. כך למשל, מערכות מידע לתושב כמו דיגיתל מתוכננות להתפתח ולכלול מודולים לזיהוי ההתנהגות העתידית של התושב. כפי שמתאר זאת זהר שרון, מנהל מנהלת הידע העירוני בעיריית תל־אביב,

"וכאן אנחנו בתל־אביב מנסים לדחוף את זה יותר ויותר ל־ prediction. זאת אומרת, לא רק לנתח נתוני עבר של הלשכה המרכזית לסטטיסטיקה שהיו נכונים לפני שנתיים, אלא ננהל נתונים בזמן אמת וננתח אותם ונגיע למצב כזה של אנליזות בצורה כזאת שנוכל מראש לתת שירותים טובים יותר, לעשות מניעה טובה יותר... זה משהו שלדעתי ילך ויגבר בצורה מאוד משמעותית בניהול החכם של העיר".¹⁶

• **סטנדרטיזציה של טכנולוגיות העיר בעידן הדיגיטלי.** תשתיות דיגיטליות הן יקרות מאוד לפיתוח, בעיקר כאשר אין מערכות סטנדרטיות בשוק, באותו האופן שבו מערכות ERP הן סטנדרטיות בשוק הארגוני.¹⁷ ליאורה שכטר, מנהלת אגף מחשוב ומערכות מידע בעיריית תל־אביב מתארת מגמה זו כך:

"בהרבה ערים עולה צורך מצד המנמ"רים בעזרה וסיוע של ההנהלה בעיקר בסוגיות משאבים כדי לקדם מערכות. ישנה אמירה, שחוזרת ונשנית, 'אנחנו לא יכולים לעשות את מה שתל־אביב עושה, מפתחת מערכות באופן עצמי'. רוב העיריות אינן מפתחות בעצמן, הן נסמכות על פתרונות של חברות חיצוניות. כאשר בכל התקשרות נדרש לצאת למכרז – ולכן מארג של אינטרסים שצריך לטפל בו. העולם הוא לא אוטופי, בכל סיטואציה של תהליכי פיתוח יש דרכים להתמודד בפן האינטגרטיבי, שזה מה שנדרש מאיתנו בעת הזו! למשל: לשקף לתושב את מצבו בכל תחומי העיסוק של העירייה (חינוך, רווחה, קהילה, חנייה, ארנונה) – מאחר והשליטה בפיתוח המערכות הינה עצמאית בתל־אביב, אני יכולה ליצור אזור אישי שבו יש אינטגרציה בין כל התחומים. אם עירייה שוכרת מגוון חברות, האחת למערכת ארנונה ואחרת לחנייה ואחרת למשהו אחר, יהיה לה אתגר גדול בהרבה ליצור אינטגרציה. אם נצליח להביא את השוק לפיתוח של ERP נצמד לקראת עידן של שירות אינטגרטיבי".¹⁸

15 יוסי בן סימון (מנמ"ר, עיריית אשדוד), 25.9.2016.

16 זהר שרון (מנהל מנהלת הידע העירוני, עיריית תל־אביב), 10.8.2016.

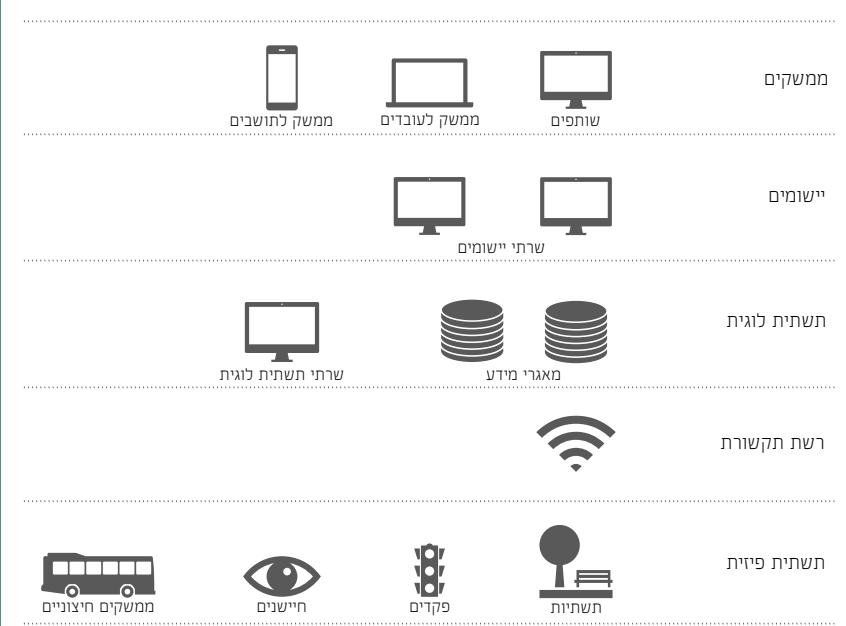
17 מערכות ERP (Enterprise Resource Planning) הן מערכות המנהלות תהליכי ייצור, מכירות, כוח אדם ולמעשה כל תהליך ארגוני ברוב סוגי הארגונים הגדולים במשק.

18 ליאורה שכטר (מנהלת אגף מחשוב ומערכות מידע, עיריית תל־אביב), 1.11.2016.

רוב הטכנולוגיות המתוארות שייכות לקטגוריה הראשונה, כלומר פרויקטים המופעלים בידי העיריות (כך למשל פרויקט דיגיתל של עיריית תל־אביב), אך יש גם דוגמאות יוצאות מן הכלל. כך למשל, יהוד מרסיאנו, ראש אגף חדשנות ומערכות מידע בעיריית באר שבע, נותן דוגמאות לגישת ה־ bottom-up:

"יש תושבים שעושים בעצמם שכבות של מידע. למשל, יש לנו פה תושב שעשה שכבה של שבילי אופניים. הוא הלך ומיפה – יחד עם עוד אנשים – את כל שבילי האופניים בעיר... אנחנו גם מאמינים שאפשר לתת את הכוח לתושבים לייצר דברים כלשהם, שאחר כך גם תושבים אחרים יכולים להשתמש [בהם] וגם אפילו העירייה יכולה להשתמש [בהם]".¹¹

לטכנולוגיות המוטמעות כיום בערים כמה מאפיינים טכנולוגיים נפוצים. לפני הכול, חלק גדול מן היישומים נשענים על טכנולוגיות IoT (Internet of Things)¹² כתשתית המקשרת בין הסביבה הפיזית למערכות המידע. תשתית זו כוללת חיישנים מחוברים, פקדים ורכיבי תקשורת המקשרים בין כל החלקים השונים. התשתיות הפיזיות הנפוצות ביותר כוללות מצלמות אבטחה וניהול עירוני וכן חיישנים בפחי אשפה. התשתית מחוברת בכמה סוגים של רשתות תקשורת – כבלי נחושת, כבלים אופטיים, רשתות Wi-Fi, רשתות סלולר ו־Fog Networks.¹³ הפרוטוקולים הנפוצים הם SCADA,¹⁴ בעיקר לתשתיות פיזיות ותיקות יותר, או רשת האינטרנט. תרשים 2.1 מתאר כיצד יישומים שונים נראים ברמות הטכנולוגיה השונות. מערכות כגון תחבורה ברמת התשתית הפיזית מתקשרות בעזרת רשת התקשורת עם התשתית הלוגית, האוגרת מידע והמאפשרת ליישום לפעול מול התשתית הפיזית או מול הממשקים לתושבים ולמשתמשים אחרים.



11 יהוד מרסינו (מנהל אגף חדשנות ומערכות מידע בעיריית באר שבע), 15.9.2016.

12 "מְרֻשֶׁת הֶדְבָּרִים" (באנגלית: "Internet of Things", או בקיצור IoT), היא רשת של רכיבים פיזיים, המשובצים בחומרה ובתוכנה והמחברים את הרכיבים לרשת האינטרנט ולרכיבים אחרים.

13 "רשת ערפל" או "מחשוב ערפל" (ובאנגלית: "Fog Networks") הוא מודל של רשת, שבו עיבוד המידע מתבצע ברכיבים המקושרים עצמם ולא במחשוב הנגיש דרך האינטרנט.

14 פרוטוקול SCADA (Supervisory Control and Data Acquisition) הוא פרוטוקול שמקורו במערכות תעשייתיות, המאפשר תקשורת עם חיישנים ועם רכיבים אחרים בעיר הדיגיטלית.

תרשים 2.1 מגוון היישומים ברמות הטכנולוגיה השונות

ניתוח הראיונות שנערכו מצביע על הבדלים גדולים מאוד בין ערים בתחום המוכנות להתקפות סייבר. ערים בעלות תשתית חזקה של מערכות מידע מסוגלות להעמיד מערכות ופתרונות הנמצאים בחזית הטכנולוגיה והנהלים הארגוניים.

עם התפתחות התשתיות הדיגיטליות בעיר גוברים הקולות המצביעים על הסכנות שבהתקפות סייבר על העיר.¹⁹ כמה התקפות על תשתיות ערים מדגימות את הסכנות הגלומות במערכות אלו. כך למשל, על פי מספר דיווחים בעיתונות ההתקפה על מנהרות הכרמל בחיפה השביתה תשתית תחבורה חשובה. על פי הפרסומים הרבים (שחברת כביש חוצה ישראל הכחישה) סוס טרויאני הצליח לחדור למערך מצלמות האבטחה במנהרות הכרמל ולהביא לשיבושים קשים ולסגירה של הכביש במשך כיומיים.²⁰ פרסומים אחרים מדווחים על מתקפות על מערכת המים בחיפה.²¹ דוח מבקר המדינה משנת 2017 באשר לחמש מועצות מקומיות חושף מקרים רבים של פגיעה בעקבות פריצות למאגרי מידע.²² כך למשל, בחודש אוגוסט 2016 נפגע שרת ששימש את מחלקת ההנדסה שבנצרת עילית, לאחר פתיחת קובץ בדואר האלקטרוני. התוקף, ששלח את הווירוס בדואר אלקטרוני, דרש מהעירייה לשלם כופר בסך 10,000 שקלים לשם הסרת מגבלת הגישה לקבצים, והיא בחרה שלא לשלמו. בהיעדר המידע בשרת נפגעה יכולת העירייה להגיש כתבי אישום נגד עברייני הבנייה.²³ מקרים אלו מחדדים את הפגיעות של העיר בעידן הדיגיטלי, ואת היכולת לשתק תשתית פיזית בעיר או לפגוע במאגרי מידע.

ניתוח הראיונות שנערכו מצביע על הבדלים גדולים מאוד בין ערים בתחום המוכנות להתקפות סייבר. ערים בעלות תשתית חזקה של מערכות מידע מסוגלות להעמיד פתרונות ומערכות הנמצאים בחזית הטכנולוגיה והנהלים הארגוניים. דוגמאות לכך נמצאות בתיאור ההיערכות שבדבריה הבאים של ליאורה שכטר:

"מה הנוזק/האיום החמור ביותר שיכול לקרות בעירייה? בעיני זה זליגת ו/או גניבת מידע על התושב. אנחנו מבצעים בימים אלו סקר סיכונים גדול שיבדוק מה הנכסים הקריטיים שלנו ומהי רמת הסיכון. מיסדנו מחדש לפני כשנה את תקני יחידת אבטחת המידע והסייבר שלנו, הכוללת כ-13 איש רק ביחידה זו, כאשר לכל עובד התמחות פרקטית בתחום - מניהול FW, ניטור אירועי אבטחה, Honey Pots. הצוות בסיוע של מומחים ייחודיים מבחוץ, יכול להתמודד עם אירוע תקיפה. לא אחת, הצלחנו לבודד וירוס חדש, לנתח את ההתנהגות, ואף לשלוח את האבחון לחברות האבטחה הגלובליות להוצאת עדכון. חשוב להבין כי זה עולם שמתפתח כל הזמן, צריך לדעת לזהות את החולשות של עצמך ולהתגונן. עשינו מהלך גדול של רישום מאגרי המידע מול משרד המשפטים, לאור הכניסה של העדכון לתקנות הגנת הפרטיות. למרות הקושי הרב ביישום, אנו מקבלים את התקנות באהבה רבה. יחד עם זאת חשוב להבין כי הרשויות לא יוכלו להחיל ברגע את כל התקנות, נדרש למדרג את היישום".²⁴

19 A.Bartoli et al., "Security and Privacy in Your Smart City," in *Proceedings of the Barcelona Smart Cities Congress* (2011); A. S. Elmaghraby and M. M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy," *Journal of Advanced Research* 5, no. 4 (2014): 491-497; Rob Kitchin, "The Real-Time City? Big Data and Smart Urbanism," *GeoJournal* 79, no. 1 (2014): 1-14

20 אי"פי והארץ, "אי"פי: השיבושים במנהרות בכרמל - בשל מתקפת האקרים, **הארץ**, 27.10.2013, <https://www.haaretz.co.il/captain/net/1.2150513>; אחיה ראב"ד ו' AP, "מנהרות הכרמל נסגרו עקב מתקפת האקרים, **ynet**", 27.10.2013, <https://www.ynet.co.il/articles/0,7340,L-4446249,00>.html

21 כתבי ynet, "ארגון סורי ערך מתקפת סייבר נגד מערכת המים, **ynet**", 25.05.2013, <https://www.ynet.co.il/articles/0,7340,L-4383924,00.html>.

22 מבקר המדינה, "דוחות על הביקורת בשלטון המקומי לשנת 2017", 21.11.2017, [http://www.mevaker.gov.il/\(X\(1\)S\(ckekgop4frdnngarvasl4iz\)\)/he/Reports/Pages/610.aspx?AspxAutoDetectCookieSupport=1](http://www.mevaker.gov.il/(X(1)S(ckekgop4frdnngarvasl4iz))/he/Reports/Pages/610.aspx?AspxAutoDetectCookieSupport=1).

23 אילן ליאור, "מבקר המדינה: מאגרי מידע רגישים ברשויות המקומיות חשופים להתקפות סייבר, **הארץ**", 21.11.2017, <https://www.haaretz.co.il/news/politi/premium-1.4619758>.

24 ליאורה שכטר (מנהלת אגף מחשוב ומערכות מידע, עיריית תל-אביב), 1.11.2016.

לעומת זאת איציק כרמלי, מנמ"ר עיריית ראשון לציון ומרכז תוכנית עיר חכמה, מתאר מציאות בעייתית בערים אחרות:

"כרגע אף רשות לא מונחת במטה הסייבר, זה אומר שיכולה להיות רשות אפילו בלי שום מנגנון אבטחת מידע, אפילו לא אנטי-וירוס. אין הנחיה, אף אחד לא מונחה ואף אחד לא בודק. בתור נציג המנמ"רים בכנסת הסברתי למטה הסייבר שברגע שתהיה בעיה, חדירה לאחת הרשויות, הבעיה תהיה ארצית, לא רשותית. יגנבו פה כספים וחדירה למערכות. עיריית ראשון לציון סולקת מיליארד וחצי שקל, צריך להבין שאלו מערכות מאוד מאוד כבדות. צריך לתת את הדעת על העניין הזה. רשות שהמנמ"ר שלה לא מספיק מבין באבטחת מידע, אין אבטחה".²⁵

מהו הבסיס החוקי והארגוני לאבטחת מידע בעיר?

ישנה חובה חוקית להגנת הפרטיות של התושבים ושל אזרחים אחרים שנשמר מידע עליהם. ברשויות המקומיות ישנם מאגרי מידע רבים, המשמשים בסיס לעבודתן בתחומים רבים, והם כוללים ענייני כספים, חינוך, רווחה, תכנון ובנייה וכן הלאה. מגמת הערים החכמות מביאה לגידול מערכתי בכמות הנתונים שבידי הרשויות המקומיות ובמספר מסדי הנתונים שהן מפעילות. פגיעה במערכות הממוחשבות ובמאגרי המידע של הרשויות המקומיות עלולה לגרום לנזקים כבדים, ובכלל זה לפגיעה בשירותים הניתנים לתושבים ולפרטיות המידע על אודותיהם, ולכן מושלת עליהן החובה להגן על המידע. נושא זה קשור לפרטיות המידע,²⁶ ובייחוד לזיקה שבין הפרטיות לבין אבטחת המידע. אבטחת מידע היא קריטית להבטחת פרטיותם של התושבים ולבטיחותם האישית, ולכן היא תנאי לקיום הוראות חוק הגנת הפרטיות וחוקים אחרים. כפי שכותב מבקר המדינה,

"היות שמאגרי המידע מכילים פרטים אישיים, ומסירת נתונים על אדם לזולת עלולה לפגוע בפרטיותו, יש לאבטח את המידע. ככל שאדם עלול להיפגע יותר מגילוי המידע עליו ברבים, עולה רמת רגישות המידע ועמה רמת האבטחה שיש לנקוט כדי לשמור עליו. חוק הגנת הפרטיות מגדיר 'אבטחת מידע' - כ'הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין'. החוק קובע כי 'בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע'.²⁷

המאפיינים של ערים בעלות תשתיות דיגיטליות חושפות אותן להתקפות ייחודיות, מעבר להתקפות הסטנדרטיות על מערכות מידע המחוברות לאינטרנט, כגון התקפות על רשת התקשורת. תרשים 2.2 מדגים את נקודות התורפה הרבות של העיר בעידן הדיגיטלי.

התשתית הדיגיטלית בעיר מהווה נקודת תורפה גדולה, בגלל הפגיעות של רכיבי IoT, רשתות SCADA או רשתות אלחוטיות. ההטמעה של התשתיות הדיגיטליות בעולם הפיזי מאפשרת להתקפות על העיר להיות אפקטיביות הרבה יותר ומסוכנות, לפחות פוטנציאלית. זאת ועוד, הממשקים הרבים שיש לעיר עם התושבים ועם העובדים חושפים את העיר להתקפות רבות. התקפות על הגורם האנושי במערכות מידע הופכות להיות בעלות משמעות יותר ויותר באבטחת מידע. לכן העובדה שמערכות דיגיטליות מתקשרות עם תושבים בעזרת יישומונים בטלפונים חכמים, מחשבים בבתי ספר ובאזורים ציבוריים ומחשבים המיועדים לעובדים מגדילה את חזית הפגיעה האפשרית בעיר. לבסוף, האינטגרציה של מאגרי המידע מגדילה את הסיכון לפגיעה בפרטיות התושבים והופכת את מטרות העיר הדיגיטלית למעניינות יותר להתקפה.

25 איציק כרמלי (מנמ"ר ומרכז תוכנית עיר חכמה, עיריית ראשון לציון), 8.9.2016.

26 ראו הרחבה בפרק 4.

27 מבקר המדינה, "אבטחת מידע והגנת פרטיות ברשויות המקומיות", (מעקב מורחב - דוח ביקורת שנתי מס' 62, 2012), 2017.

איומים על תשתיות דיגיטליות

כדי להבין את האיומים יש לבחון את רמות הטכנולוגיה בעיר ואת אופן הביטוי של כל איום ברמות השונות. האיומים מופנים כלפי יישומים, מסדי נתונים, תשתיות לוגיות, תשתיות פיזיות ורכיבי תקשורת.²⁸ האיומים המשמעותיים ביותר הם האיומים שנגרמים בכוונת מכוון והכוללים התקפה, ציתות למידע, גניבת מידע, שינוי מידע וגישה לא־מורשית. בשורות הבאות ייסקרו האיומים המרכזיים.

חבלה – מתבטאת בשיבוש של מערכות העיר באמצעות פגיעה ברכיבי תוכנה או חומרה או במערכות מידע המנהלות את התשתית. מערכות פגיעות במיוחד הן מערכות שהן קריטיות למהלך החיים בעיר. תשתית אנרגיה, מים, תחבורה, תקשורת, בנקאות וביוב הן אולי המערכות הקריטיות ביותר. בהתקפות אלו מטרת התוקף היא להפסיק או לשבש בצורה רצינית את פעולת המערכות, או אף להפעיל את המערכות בצורה שתגרום לנזקים שאינם ניתנים לתיקון. כיוון שבערים חכמות השליטה בתשתיות פיזיות כגון תשתיות מים, אנרגיה ותחבורה היא בעזרת מערכות מידע, התוצאה הפוטנציאלית של התקפות שכאלו יכולה להיות קשה.

איומים כגון אלו עלולים להתממש באמצעות חדירה למחשבי מערכות המידע שמנהלים את המערכות, כפי שקרה בהתקפה על תשתית החשמל בקייב שבאוקראינה בסוף שנת 2016.²⁹ דוגמה מקומית יותר היא הטענה שפורסמה בתקשורת הישראלית, ולפיה ארגון סורי צבאי למחצה הואשם בהתקפות על תשתיות דיגיטליות בחיפה.³⁰ שיטה נוספת היא התקפות מסוג של Distributed Denial of Service (DDoS), המכוונות בראש ובראשונה נגד מחשבים המחוברים לרשת האינטרנט, ובהן מציפים נתבים ורכיבים נוספים בקריאות רבות כל כך עד שהרשת קורסת תחת העומס או מפסיקה באופן יזום את השרות.

המניע לחבלות יכול להיות כלכלי. כך למשל, מחשבים במערכת החינוך של עיריית חוף אשקלון הותקפו בידי וירוס כופר, והעירייה שילמה עשרות אלפי דולרים כדי לשחרר אותם.³¹ גם כאן, מאחר שתשתית מחשוב שהעירייה מפעילה – בבתי ספר או במקומות אחרים – היא קריטית, כך גם האיומים עליה יכולים להיות גדולים מאוד.

גניבת מידע – מתמקדת בגישה לא־מורשית למאגרי מידע, לקבצים או לטכנולוגיה. גניבת מידע יכולה להשפיע על פרטיות התושבים ועל כל האנשים שעליהם העיר שומרת מידע (יוממים, עובדים, מבקרים ותיירים). גניבה יכולה להתבצע בפענוח תקשורת מוצפנת או לא־מוצפנת, בחדירה לרשת המחשבים ואף בגניבה פיזית של מחשבים. כיום עיריית אוספופ ומתחזקות מאגרי מידע הולכים וגדלים. מאגרים אלו כוללים אינטגרציה של היבטים שונים (ורגישים) של חיי התושבים וכן מידע ממערכות חינוך, רווחה ותחבורה, מאפיינים אישיים, נתוני דת ועוד. לדברי ברק שחר, מנהל מערכות תקשוב במרכז השלטון המקומי,

"ברשויות המקומיות ישנם מאגרי מידע רבים, חלקם מכילים מידע אישי רגיש על אזרחים, לכן לא פלא שתוקפי סייבר ישאפו לפרוץ למאגרים אלה. ככל שאנו מתקדמים לכיוון של עיר חכמה בארץ ובעולם, האיומים רק גוברים, הן על מערכות

28 European Union Agency for Network and Information Security, "Cyber Security for Smart Cities – An Architecture Model for Public Transport," 2015, https://www.enisa.europa.eu/publications/smart-cities-architecture-model/at_download/fullReport

29 Andy Greenberg, " 'Crash Override': The Malware that Took Down a Power Grid," *Wired*, December 6, 2017

30 ראו כתבי ynet, "ארגון סורי",

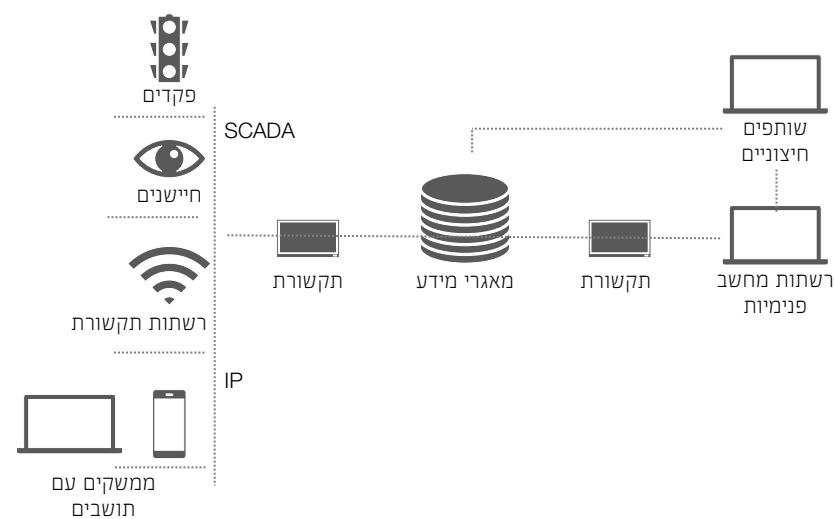
31 ניקי גוטמן, "מועצה אזורית שילמה כופר להאקרים," *ישראל היום*, 25.04.2018, <http://www.israelhayom.co.il/article/551377>

מידע והן על מערכות ממוחשבות השולטות בתשתיות קריטיות המשמשות את האזרחים ומאפשרות חיים תקינים במרחב האורבני.³²

לפיכך, לא מפתיע כי המאגרים הם יעד להתקפות חיצוניות ופנימיות. המקור להתקפות חיצוניות הוא האקרים (פצחנים), המנסים לחדור למאגרי המידע מחוץ למערכות המחשוב.

גישה לא־מורשית – מאגרי מידע הם גם כר פורה לפריצות של גורמים פנימיים כגון עובדי עירייה, שמשתמשים בגישה למאגרים גם לצרכים שאינם מורשים. כך למשל, עובדים ברשויות שונות כגון הביטוח הלאומי, רשות המיסים ובזק הואשמו בגניבת מידע ממאגרים ומכירתו לחוקרים פרטיים.³³ גישה לא־מורשית יכולה לכלול העתקה של המידע או שינויו, כך למשל כדי למחוק דוח שנתן הפיקוח העירוני.

תקלות ותאונות – אף שהדיון באבטחת מידע נוטה להתמקד באיומים שבהם ישנו תוקף (חיצוני או פנימי), איומים חמורים במיוחד נובעים מתאונות ומתקלות דווקא. תקלות בחומרה, בתכנות המערכות, בתיאום בין מערכות או ברשת התקשורת יכולים להביא להפסקת הפעילות או לשיבושים קשים בשירותים קריטיים. מאחר שבעיר הדיגיטלית מתחזק החיבור שבין תוכנה לתשתיות הקריטיות בעיר, הרי לתקלות, לבאגים ולתאונות עלולות להיות תוצאות חמורות. החוקרים דודג' וקיטשין טבעו את המושג קוד/מרחב (code/space) כדי לתאר מרחבים פיזיים שקשורים בקשר הדוק לתוכנה, כך שהמרחב אינו יכול לתפקד אם התוכנה אינה מתפקדת כמתוכנן.³⁴ אם למשל התוכנה המפעילה את הרמזורים בעיר מפסיקה לעבוד, התנועה בעיר תיעצר. לפיכך אם התהליך של בניית המערכות אינו מנוהל באיכות הדרושה, לערים חכמות יש פוטנציאל ליצור "ערי באגים", שבהן יש תקלות הולכות ונשנות.



32 ITPortal, "ערים חכמות תחת מתקפה," 31.12.2017, הפקתם-תחת-תומכה-סירע <http://itportal.co.il>

33 אבי כהן, "בכירים בביטוח לאומי ורשות המס סחרו במידע," *ynet*, 6.9.2006, <https://www.ynet.co.il/articles/0,7340,L-3300295,00.html>

34 Kitchin, "The Real-Time City?"

ברשויות המקומיות ישנם מאגרי מידע רבים, חלקם מכילים מידע אישי רגיש על אזרחים, לכן לא פלא שתוקפי סייבר ישאפו לפרוץ למאגרים אלה.

תרשים 2.2 נקודות התורפה של העיר בעידן הדיגיטלי

האיומים הגדולים ביותר הם האיומים שנגרמים בכוונת מכוון והכוללים התקפה, ציתות למידע, גניבת מידע, שינוי מידע וגישה לא־מורשית.

הפתרונות לאיומים שמולם ניצבת העיר הדיגיטלית כוללים הפעלה של תהליכי תכנון, בנייה ותחזוקה נכונים והטמעה של תרבות של אבטחה מידע בכל רמות הארגון. ישנן פרקטיקות רבות המקובלות בעולם אבטחת המידע. בשורות הבאות מובאת רשימת המלצות המתמקדות באיומים על העיר הדיגיטלית. ההמלצות מאורגנות כך שתחילה מובאים פתרונות טכנולוגיים סטנדרטיים למימוש ולאחריהם פתרונות מורכבים יותר, הדורשים מאמצים ארגוניים ולא רק טכנולוגיים.

פתרונות טכנולוגיים

- **הצפנת מידע.** הצפנת מידע הופכת נתונים ומידע לקוד הדורש מפתח כדי לפענחו. ככלל אין סיבה שמידע כלשהו בעיר לא יהיה מוצפן, בעיקר כאשר הוא עובר בקווי תקשורת, אך גם כאשר המידע נשמר במאגרי המידע של העירייה, של חברות שונות ובמחשבי העובדים.
- **שימוש ברשתות פרטיות.** ככלל, תשתית התקשורת והתפעול של העיר צריכה להתבסס על רשתות תקשורת פרטיות, המופרדות מרשת האינטרנט באמצעות הפרדה פיזית או וירטואלית. השימוש ב־Virtual Private Networks (VPN) מאפשר ליצור רשת וירטואלית, המשתמשת בהצפנה ובהגבלת גישה כדי להפריד את זרימת המידע מרשתות אחרות.
- **שימוש באמצעי אבטחה.** בכל מערכת ורשת הקשורות לעיר יש להשתמש באמצעים כגון Firewalls, Malware Detection Systems, Network Intrusion Systems, DDoS Protection וכן הלאה. יש לתכנן כיצד הכלים השונים משתלבים ומעניקים הגנה מלאה לתשתיות ולמערכות.
- **הגנה על התשתית הפיזית.** יש להגן על התשתיות הפיזיות של העיר ולוודא, כי אין אפשרות להחליף רכיבים המותקנים בשטח וכי מחשבים והתקנים השייכים לעובדים ולחברות המתפעלות מוגנים.
- **בדיקה מקיפה של המערכות.** יש להטמיע תהליכי עבודה, שלפיהם כל המערכות המוטמעות בעיר נבדקות תדיר – בזמן התכנון, בעת ההטמעה ובצורה סדירה לאחר מכן. הבדיקות צריכות להיעזר בשיטות מתקדמות לבחינה, לרבות סקרי סיכונים, בדיקות חדירה (Penetration Testing) ו־Bug Bounties.
- **הגבלה של מידע שנאסף מהמשתמשים.** כל מידע נוסף הנאסף מן התושבים או מן המשתמשים האחרים של העיר יכול להיות מטרה לתקיפה או לגניבה. לפיכך – וגם מסיבות הקשורות לפרטיות – יש לוודא כי נאסף המידע המינימלי הנחוץ לאספקת השירות.
- **בקרה ופיקוח לוגיים.** יש לוודא כי כל מערכת בעיר מבוקרת בקביעות בידי מי שמונו לשם כך כדי לזהות אם יש פעולות חריגות אשר גורמים שאינם מורשים ביצעו או ניסו לבצע. יש לבצע רישום מדויק של כל גישה למאגר מידע או למערכת, של המידע שנקרא ושל המשתמשים שביצעו את הפעולות.
- **גיבוי והתאוששות מאסון.** יש לוודא כי כל המידע הנאסף בעיר וכל המידע המשמש לקבלת החלטות ולפעולות מגובה בצורה המאפשרת התאוששות מהירה מאסון.

פתרונות ארגוניים

- **תרבות ארגונית של אבטחת מידע.** ישנה חשיבות ליצירה של תרבות ארגונית המונחית לאבטחת מידע והכוללת אבטחה עמוקה, ובה שכבות רבות של אמצעי אבטחה המגינים על האלמנטים הרגישים בעיר. תרבות מונחית אבטחה צריכה להתחיל לפני תכנון המערכות בעיר, ולא להתווסף מאוחר יותר. תוכניות מודרניות לבניית ערים עם תשתיות דיגיטליות מביאות בחשבון את הגנת המידע כחלק בסיסי מבניית העיר. דוגמה מקומית נמצאת בהחלטת ממשלה משנת 2016, שלפיה יועברו כ־7.5 מיליון שקלים להפיכת חיפה לעיר חכמה מוגנת סייבר. כ־4 מיליון שקלים מהתקציב יועברו ממערך הסייבר למטרת הגנת התשתיות בעיר.³⁵
 - **בנייה של נוהלי אבטחת מידע והקפדה עליהם.** יש לתכנן ולכתוב מסמך מדיניות להגנה על מידע ועל מערכות, ולוודא כי המסמך מיושם בארגונים הקשורים לעיר. סטנדרטים שכאלו כוללים את ISO/IEC 27000,³⁶ או את NIST Cybersecurity Framework (NIST CSF).³⁷ יש לוודא כי כל עובדי הרשות, המהנדסים והמפעילים הקשורים לתשתיות דיגיטליות יעברו הדרכות וימלאו אחריהן בקפדנות. כדי למנוע Zero Day Attacks יש לוודא, כי כל המחשבים והרכיבים יהיו מעודכנים בגרסאות האחרונות של מערכות ההפעלה וכי כל טלאי האבטחה הותקנו.
 - **מינוי ממונה על אבטחת מידע.** יש לוודא, שבכל רשות מקומית או בפרויקטים חשובים ישנם ממונים בעלי הסמכה ובעלי ניסיון מתאים לתפקיד ממונה על אבטחת המידע.
 - **יצירת תרבות אבטחה בקרב ספקים.** יש לוודא כי כל הספקים המספקים תוכנה, התקנים ושירות לעיר יעמדו בסטנדרטים הנדרשים. יש לוודא זאת ביחוד כאשר להתקני IoT, שהם אחת החוליות החלשות ביותר באבטחת העיר בעידן הדיגיטלי.
- להשלמת התמונה נציין, כי מערך הסייבר הלאומי מקדם הצעת חוק, שלפיה הסמכות והאחריות לניהול סוגיות של הגנת סייבר תהיה לאומית־ריכוזית ותנוהל בידי מערך הסייבר. מהלך זה נמצא רק בראשיתו, ואין לדעת בשלב זה כיצד יתפתח.

35 אורה קורן, "חיפה תיהפך לעיר חכמה מוגנת סייבר", **TheMarker**, 28.12.2016, <https://www.themarker.com/news/macro/1.3182332>

36 ISO – International Organization for Standardization, "ISO/IEC 27000 Family – Information Security Management Systems", 2013, <https://www.iso.org/isoiec-27001-information-security.html>

37 NIST – National Institute of Standards and Technology, "Cybersecurity Framework," <https://www.nist.gov/cyberframework>

ישנה חשיבות ליצירה של תרבות ארגונית המונחית לאבטחת מידע והכוללת אבטחה עמוקה, ובה שכבות רבות של אמצעי אבטחה המגינים על האלמנטים הרגישים בעיר.