מאמר זה פורסם בכתב העת "חידושים בניהול", גיליון מס' 16, מרץ 25,
היוצא לאור על ידי הפקולטה לניהול על שם קולר באוניברסיטת תל אביב.

חומת סייבר איתנה לעיר החכמה – ייעול הקצאת תקציב עירוני לאבטחת סייבר בערים חכמות: תובנות מתל אביב והרצליה

יואב זיו שחר רייכמן יעקב מנדל

יואב זיו הוא דוקטורנט בפקולטה לניהול ע"ש קולר באוניברסיטת תל אביב. בעל תואר ראשון בהנדסת תעשייה ותואר שני בניהול מערכות מידע, שניהם מאוניברסיטת תל אביב. תחומי המחקר שלו כוללים ערים חכמות, IoT ואיומי סייבר בעידן המודרני.

ד"ר שחר רייכמן הוא חבר סגל בכיר וראש המחלקה לניהול טכנולוגיה ומידע בביה"ס לניהול ע"ש קולר באוניברסיטת תל אביב. מחקריו עוסקים בקשר בין פעילויות Online לפעילויות Offline לצורך תמיכה בקבלת החלטות עסקיות ושיפור תהליכים צרכניים. המחקרים כוללים ניתוח ועיבוד מתקדם של Big data בארגונים, בסביבות מקוונות וברשתות חברתיות, שימוש בכלי Machine learning, אקונומטריקה ושיטות ניתוח רשתות מורכבות, למציאת תבניות ומאפיינים ייחודיים המאפשרים בניית מודלים לחיזוי והסבר תהליכי מסחר מקוון. הצטרף לפקולטה לניהול בשנת 2014 לאחר פוסט-דוקטורט במכון הטכנולוגי של מסצ'וסטס (MIT). את לימודי הדוקטורט סיים באוניברסיטת תל אביב בשנת 2011.

ד"ר יעקב מנדל הוא חבר סגל בכיר בפקולטה לניהול ע"ש קולר באוניברסיטת תל אביב ומנהל את קבוצת המחקר בתחום הקריפטוגרפיה והסייבר בחברת State Street. יזם סייבר סידרתי ושימש כמנכ"ל מרכז הסייבר והמצוינות בחברת אינטל. היה אחד היזמים והמנכ"ל של חברת SCsquare שנמכרה לחברת ברודקום. בעל 23 פטנטים רשומים בתחום הסייבר, בינה מלאכותית ובלוקצ'יין. בעל ניסיון עשיר ומגוון בתחומי הסייבר, ניהול והגנה על זכויות יוצרים, בדיקות חדירות ופתרונות סייבר לרשתות חכמות. תחומי מחקריו הם: ההיבטים הכלכליים של מתקפות סייבר, PQC, MPC, FHE המשכיות הפעילות העסקית תחת התקפות סייבר על הארגון, טכנולוגיית בלוקצ'יין (פרוטוקולים מתקדמים, היבטי פרטיות, מערכות תשלומים חדשות) וקוונטום.

תקציר

בעידן דיגיטלי המתאפיין בשילוב מהיר של טכנולוגיה בסביבות עירוניות, ההכרח לאבטחת תשתיות דיגיטליות גדל באופן משמעותי. האינטגרציה ההולכת וגוברת של טכנולוגיות הערים החכמות ומערכות האינטרנט של הדברים (IoT) הובילה למנעד רחב חדש של איומי סייבר. בשנים האחרונות ניתן לראות עלייה במתקפות סייבר המכוונות לערים, תוך ניצול פגיעות בטכנולוגיות חכמות כדי לשבש שירותים קריטיים ולסכן את התושבים. מציאות זו מדגישה את הדחיפות בשמירה על תשתיות דיגיטליות במסגרות עירוניות.

מחקר זה עוסק בדינמיקה המורכבת של הקצאת תקציב עירוני לאבטחת מידע בהקשר של ערים חכמות מתפתחות. המחקר מתמקד בעיריות תל אביב והרצליה בישראל כמקרי בוחן, ומטרתו לחשוף דפוסים ויחסים המעצבים החלטות תקציביות. מתוך מערכי נתונים מקיפים הכוללים ספרי תקציב, מצבת כוח אדם, אוכלוסיית הערים וחומרת אירועי סייבר על פני תקופה של חמש שנים, המחקר מספק תובנות לגבי המתאמים בין משתנים אלה והשלכותיהם על מוכנות אבטחת הסייבר. תובנות ממערכי נתונים מקיפים חושפות מתאם בין החלטות תקציביות, דינמיקה של אוכלוסייה וחומרת אירועי סייבר, תוך הדגשת אסטרטגיות לשיפור המוכנות לאבטחת סייבר.

מבוא

על פי תחזיות האו"ם, 70% מאוכלוסיית העולם תתגורר בסביבות עירוניות עד 2050, נתון המשקף את האתגרים הגדולים שעימם עיריות מתמודדות כיום ויידרשו להתמודד גם בעתיד. תהליך העיור מעלה סוגיות מורכבות כמו אי שוויון, דאגות בריאותיות, זיהום ודרישות תשתית (Feachem et al., 1989; Kuddus et al., 2020; Mcmichael, 2000; United Nations, 2018). כדי להתמודד עם אתגרים אלה, ערים פונות יותר ויותר לפתרונות מבוססי טכנולוגיה, ובהם רעיון "הערים החכמות" שמטרתו לשפר את החיים העירוניים באמצעות חדשנות ויעילות.

האבולוציה של ערים חכמות מעוררת עניין עולמי בשנים האחרונות, במיוחד בהקשר של שילוב הטכנולוגיה במגזרים שונים כגון כלכלה, תחבורה, ביטחון, אנרגיה, בריאות וסביבה (Ricciardi & Za, 2014). יוזמות העיר החכמה רותמות טכנולוגיות מתקדמות כמו בינה מלאכותית (AI), נתוני עתק (Big Data), האינטרנט של הדברים (IoT) ולמידת מכונה (Machine Learning) כדי לאסוף ולעבד נתונים לקבלת החלטות מושכלות ולשיפור הענקת השירותים המוניציפליים (Bogdoll et al., 2021; Gaur et al., 2015; Kusumawati et al. , 2017).

עם זאת, לצד היתרונות באימוץ הטכנולוגיות, מגיעים גם סיכוני אבטחת סייבר משמעותיים. תשתיות של עיר חכמה פגיעות לאיומי סייבר שעלולים לשבש שירותים חיוניים ולהוות סיכונים לביטחון הציבור (Andrade et al., 2020; Elmaghraby & Losavio, 2014; F. Khan et al., 2021). הדבר מחייב אמצעי אבטחת סייבר חזקים, אך עיריות רבות מתמודדות עם אילוצים תקציביים ומתעדפות הוצאות אחרות על פני אבטחת הסייבר (Washburn et al., 2009; Cerrudo & Spaniel, 2015; Mondschein et al., 2020).

האינטרנט של הדברים, העיר החכמה ומה שביניהם

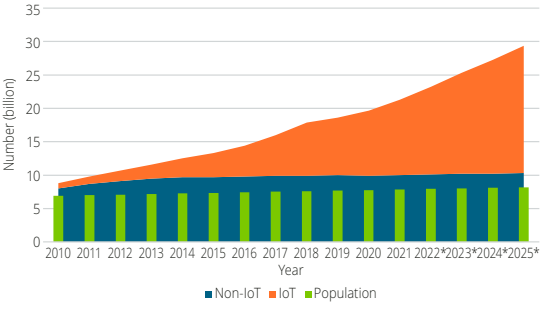
האינטרנט של הדברים (IoT – Internet of Things) מתאר רשת של מכשירים פיזיים המחוברים לאינטרנט, ומאפשרים איסוף, שיתוף וניתוח נתונים באופן אוטומטי. מכשירים אלו יכולים להיות חיישנים, מצלמות, אורות, רמקולים, או אפילו מכשירי חשמל ביתיים, שמטרתם לשפר את היעילות, הנוחות והאינטגרציה בין מערכות שונות.

השימוש בטכנולוגיות IoT הוא אחד היסודות המרכזיים של ערים חכמות, שכן הוא מאפשר איסוף וניתוח של נתונים בזמן אמת כדי לייעל ניהול משאבים עירוניים כמו תחבורה, תאורה, אנרגיה ואפילו שירותים ציבוריים. עם זאת, יישום IoT כשלעצמו לא הופך עיר ל"חכמה" בהכרח. המשמעות האמיתית של עיר חכמה טמונה ביכולת לשלב את הנתונים שנאספו באמצעות IoT בגישות מונחות נתונים (Data-Driven Approaches) כדי לייצר תובנות, לשפר תהליכים ולקבל החלטות מושכלות. ללא השימוש בגישות מונחות נתונים, יישום IoT עשוי להוות

תשתית יעילה אך חסרת תועלת אסטרטגית אמיתית. העיר לא תנצל את הפוטנציאל הטמון במידע שנאסף כדי לקדם מטרות כמו קיימות, שוויון או איכות חיים משופרת לתושבים. לכן IoT הוא אומנם כלי מרכזי בעיר חכמה, אך חייב להיות משולב בגישות הממוקדות בנתונים כדי לממש את החזון הכולל של עיר חכמה.

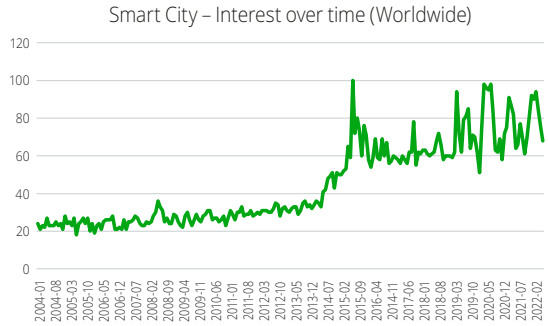
כאמור, ניתן לתאר קשר אינטגרלי בין IoT לערים חכמות, כשטכנולוגיית IoT מניעה איסוף נתונים, בקרה ואבטחה בתוך מערכות עירוניות. ערים חכמות ממנפות את ה-IoT כדי לשפר את קבלת ההחלטות, איכות השירות והעצמת האזרחים באמצעות שילוב נתונים בזמן אמת. כפי שניתן לראות באיור 1, הצמיחה של ה-IoT צפויה להמשיך לעלות באופן מעריכי, עם צפי ל-30 מיליארד מכשירים מחוברים עד 2030, בהיקף העולה בהרבה על נתוני האוכלוסייה העולמית.

איור 1: מספר מכשירי ה-IoT, מכשירי ה-Non-IoT והאוכלוסייה העולמית (Transforma Insights, 2020, 2022)



במקביל, טכנולוגיות הערים החכמות, שתפסו תאוצה בשנים האחרונות (כפי שניתן לראות באיור 2), מציעות יתרונות רבים על ידי מינוף ניתוח הנתונים, למידת תובנות, וכן בניית אוטומציות מוניציפליות כדי לייעל סביבות עירוניות. טכנולוגיות אלו משפרות את התחבורה, את ניהול האנרגיה, בטיחות הציבור ומעורבות האזרחים, ומטפחות חוסן וקיימות בתוך אתגרי עיור ואקלים. יישום מוצלח מחייב אבטחת סייבר איתנה, גישה דיגיטלית שוויונית ומודלים של ממשל שיתופי כדי להניע חדשנות ולהבטיח קיימות עירונית ארוכת טווח. יישומי עיר חכמה משתרעים על מגזרים מגוונים, וכוללים ממשל, תחבורה, ביטחון, כלכלה, תיירות, סביבה, קהילה, חינוך וניהול משאבים כדי לטפח מרחבים עירוניים יעילים ומותאמים למגורים ברחבי העולם.

איור 2: מגמת העניין במונח "עיר חכמה". מקור: Google Trends (ינואר 2004–אוגוסט 2022)

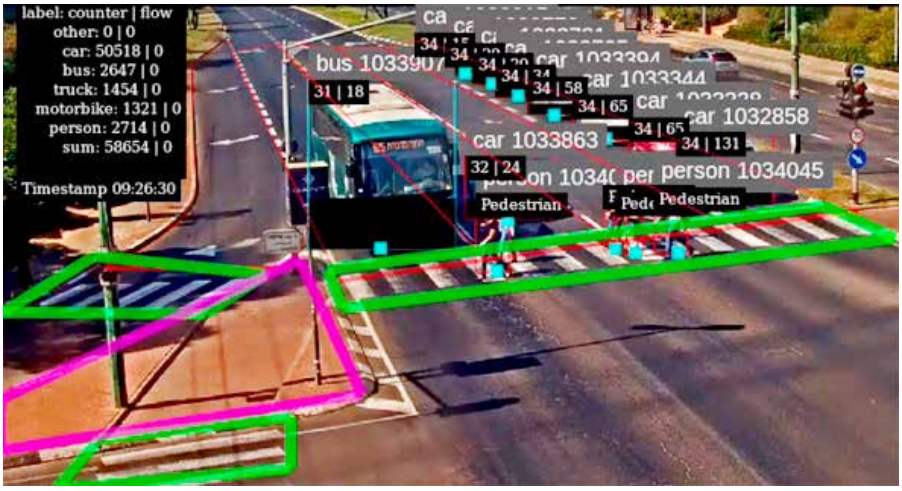


בתל אביב, לדוגמה, שילוב של רמזורים חכמים, מצלמות מעקב ומערכות תחבורה ציבורית יצר סביבה עירונית יעילה ומגיבה יותר. דוגמה למעקב תחבורתי חכם וסנכרון רמזורים, ניתן לראות באיור 3. עם זאת, מערכות אלו גם חשופות לאיומי סייבר, כפי שניתן לראות בניסיונות האחרונים לפרוץ למערכת ניהול התנועה של העיר. מקרים כאלו מדגישים את הצורך של ערים להשקיע לא רק בטכנולוגיות חכמות אלא גם באמצעי אבטחת סייבר חזקים כדי להגן על מערכות אלו מפני התקפות פוטנציאליות.

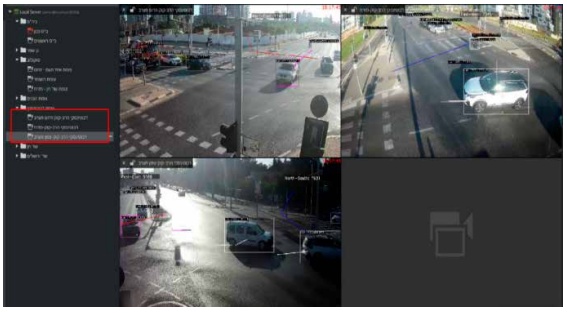
באופן דומה, בהרצליה יושמו מספר יוזמות עיר חכמה, כולל מערכות ניהול פסולת חכמות, תאורת רחוב חסכונית באנרגיה, ומערכות ניהול מים מבוססות IoT. גם בהרצליה, ניתוח תחבורה חכם מהווה אבן יסוד במיזוף "העיר החכמה", כפי שניתן לראות באיור 4. יוזמות אלו שיפרו את היעילות התפעולית של העיר והפחיתו עלויות, אך גם חשפו את העיר לסיכוני סייבר חדשים. בתגובה, עיריית הרצליה הגבירה את ההשקעה באבטחת סייבר, מתוך הכרה בצורך להגן על התשתית הדיגיטלית שלה מפני איומי סייבר. גישה פרואקטיבית זו סייעה לעיר לבנות סביבה עירונית עמידה יותר, המסוגלת לעמוד בפני אירועי סייבר ולהתאושש מהם.

עם זאת, ההתרחבות המהירה של מכשירי IoT גם מגדילה את פוטנציאל מתקפות הסייבר. ככל שהערים הופכות למקושרות יותר, הן הופכות גם לפגיעות יותר להתקפות סייבר. לדוגמה, האינטגרציה של מכשירי IoT לתוך תשתיות עירוניות קריטיות, כגון מערכות ניהול תנועה, רשתות תחבורה ציבורית ורשתות חשמל, יוצרת נקודות חדירה חדשות לתוקפי סייבר. מערכות מקושרות אלו פגיעות במיוחד להתקפות מכיוון שפריצה לרכיב אחד יכולה להשפיע על חלקים אחרים של תשתית העיר.

איור 3: מערכת ניהול תנועה חכמה (ITC), צומת נמיר-איינשטיין, תל אביב (ITC, 2022)



איור 4: ניתוח תחבורה חכמה, מבט ממצלמה, צומת הרב קוק, הרצליה (א. זיו, תקשורת בינאישית, 6 ביולי 2022)



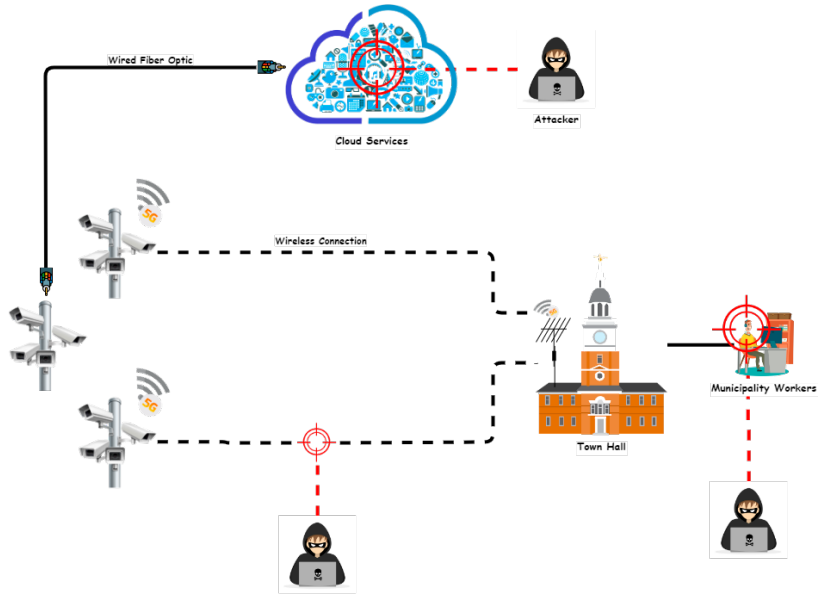
טכנולוגיות חכמות מושכות תוקפים חכמים

ככל שערים מאמצות יותר את ה-IoT וטכנולוגיות מתקדמות, כך הן הופכות פגיעות יותר להתקפות סייבר – החל ממניעת שירות (DoS), דרך פעולות של הנדסה חברתית, ועד תוכנות כופר והתקפות zero-day. לכן הטמעת מנגנוני אבטחה חזקים היא חיונית כדי להגן על נתונים רגישים ולשמור על הסודיות, השלמות והאמינות של מערכות עירוניות (Andrade et al., 2020; Elmaghraby & Losavio, 2014).

אולם מתקפה על העיר החכמה היא כמעט בלתי נמנעת, לכן בחינת נזקים ונוהלי התאוששות לאחר מתקפת סייבר חיוניים לבניית ערים חכמות עמידות. על ידי בחינת אירועי סייבר אחרונים בתל אביב ובהרצליה, כמו מתקפות DDoS, חדירה למערכות ועוד, ניתן להעלות תובנות ראשוניות לגבי האופי המתפתח של איומי הסייבר שעימם מתמודדות מערכות עירוניות. אירועים אלו מדגישים את החשיבות של אמצעי אבטחת סייבר פרואקטיביים, ניטור מתמשך ואסטרטגיות תגובה מהירה לצמצום הנזקים ולשיפור החוסן העירוני מול איומי סייבר. המערכות החכמות משלבות גם אמצעי תקשורת שונים המשמשים נקודות חדירה רגישות, כמו גם התרבות הארגונית הלוקה בחסר, כפי שניתן לראות באיור 5.

דמיינו לעצמכם את צומת הרחובות מנחם בגין-קפלן בשעות העומס. מתקפת סייבר מוצלחת יכולה להפוך את כלל הרמזורים לאדום וליצור עומסים למשך שעות רבות בעיר שגם ככה פקוקה וצפופה כמעט בכל שעות היום. יתרה מזאת, תארו לכם שהתוקף מחליט להפוך את כל הרמזורים בצומת לירוק, מצב מסוכן שעלול לגרום לפגיעה ממשית בחיי אדם.

איור 5: דוגמה למיפוי פגיעויות ברשת המצלמות החכמה של העירייה



מגוון איומי הסייבר מתפתח ללא הרף, והתוקפים מפתחים שיטות מתוחכמות יותר ויותר לניצול חולשות בתשתיות ערים חכמות. התפתחות זו מחייבת גישה דינמית לאבטחת סייבר, שבה על מנהלי הערים להתמקד לא רק במניעה אלא גם בפיתוח אסטרטגיות תגובה חזקות לצמצום ההשפעה של התקפות מוצלחות.

לדוגמה, הרצליה חוותה התקפת סייבר משמעותית בדצמבר 2020, תקיפה שהייתה מכוונת לחדירה אל שרתי העירייה באופן נרחב. עם זאת, בשל הגישה הפרואקטיבית של הרצליה לאבטחת סייבר, הצליחה העירייה לזהות את ההתקפה מוקדם וליישם אמצעים לצמצום השפעתה. אירוע זה מדגיש את החשיבות של השקעה באמצעי אבטחת סייבר חזקים כדי להגן על תשתיות קריטיות מאיומי סייבר.

תקציב מוגבל, יכולות מקצועיות נמוכות וסיכון מוגבר

עיריות רבות מתמודדות עם אתגרים משמעותיים בהקצאת תקציבים מספקים לאבטחת סייבר. למרות הסיכונים הברורים הקשורים לטכנולוגיות חכמות, ערים רבות מתעדפות הוצאות אחרות, כגון שירותים חברתיים, פיתוח תשתיות ויוזמות כלכליות על פני אבטחת סייבר. מגמה זו מוחרפת על ידי היכולות המקצועיות המוגבלות בצוותי העירייה, שלעיתים קרובות חסרים את המיומנויות המיוחדות הנדרשות לניהול מערכות אבטחת סייבר מורכבות. המחסור באנשי מקצוע שמיומנים באבטחת סייבר מקשה על ערים לנייס ולשמר את הכישרון הדרוש כדי להגן ביעילות על התשתיות הדיגיטליות שלהן.

כדי להסיק תובנות חכמות, חשוב להבין את הדינמיקה התקציבית בתל אביב והרצליה ולבחון את תהליכי קבלת ההחלטות ואת השיקולים הנוגעים להקצאת תקציבים. גם חלוקת פריטי תקציב שונים בין מחלקות העירייה וניתוח אירועי עבר הם קריטיים כדי להבין כיצד מתועדפת אבטחת הסייבר לעומת צרכים עירוניים אחרים.

בתל אביב לדוגמה, התקציב הכולל למערכות מידע גדל בהתאם לגידול באוכלוסייה, אך התקציב הספציפי לאבטחת סייבר לא הראה גידול משמעותי. הפער הזה מרמז על חוסר תעדוף של אבטחת הסייבר על רקע השקעות טכנולוגיות אחרות. האסטרטגיה של העיר נראית ממוקדת יותר בהרחבת תשתיות ושירותים דיגיטליים ללא גידול מקביל בהשקעות באבטחת סייבר, מה שעשוי לחשוף את העיר לסיכוני סייבר מוגברים.

בהרצליה, ניכרת עלייה בתקציב אבטחת הסייבר לאחר אירועי סייבר משמעותיים. הגישה הפרואקטיבית של העיר מדגישה את החשיבות של יישור ההשקעות באבטחת סייבר עם איומים

מתעוררים לשם צמצום סיכונים ושיפור החוסן העירוני. הניסיון של הרצליה מדגים את הערך של גישה מאוזנת יותר להקצאת תקציבים, שלפיה השקעות בטכנולוגיות עיר חכמה מותאמות על ידי גידול מקביל בהוצאות לאבטחת סייבר כדי להגן על השקעות אלו.

ההתפתחות המהירה של איומי הסייבר מחמירה אף יותר את התוצאות שעלולות לנבוע מיכולות מקצועיות מוגבלות. לעיתים קרובות, לעיריות חסרה המומחיות הפנימית הנדרשת כדי להתעדכן בהתפתחויות האחרונות באבטחת סייבר, מה שמשאיר אותן פגיעות לאיומים חדשים ומתפתחים. פער מיומנויות זה יכול להוביל לעיכוב בזמני התגובה, ניהול לקוי של אירועים, ולהגברת הפגיעות למתקפות סייבר.

כדי להתמודד עם אתגר זה, חלק מהעיריות ביקשו לשתף פעולה עם ארגונים פרטיים וחברות אבטחת סייבר כדי לשפר את יכולותיהן. לדוגמה, הרצליה שיתפה פעולה עם מספר חברות אבטחת סייבר כדי לבצע הערכות אבטחה שוטפות, לפתח תוכניות תגובה לאירועים, ולספק הכשרה לצוות העירוני. שותפויות אלו אפשרו לעיר לבנות פרופיל אבטחת סייבר חזק יותר ולהגיב בצורה יעילה יותר לאיומי סייבר.

טכנולוגיות חדשות, תחום חדש – תיעוד לקוי וחוסר ברגולציה

החדירה המהירה של טכנולוגיות חדשות לתחום הערים החכמות עלתה על הפיתוח של תיעוד הולם ומסגרות רגולטוריות. הפער הזה חושף את העיריות לסיכונים מוגברים ומעכב ניהול אפקטיבי של אבטחת סייבר. הניסיון של תל אביב והרצליה מדגיש את הצורך במסגרות רגולטוריות מקיפות, שקיפות מוגברת, ופרספקטיבה רחבה יותר על נוהלי הקצאת תקציב עירוני.

כיום, יוזמות רבות של ערים חכמות מנוהלות על ידי רגולציות מפוצלות, היוצרות חוסר עקביות בסטנדרטים ובנהלים של אבטחת סייבר. חוסר האחידות הרגולטורי הזה מקשה על מאמצי מנהלי הערים ליישם אסטרטגיות אבטחת סייבר מקיפות. יתרה מזאת, היעדר תיעוד מפורט של שילוב וניהול טכנולוגיות חדשות מסבך עוד יותר את יכולת הערים להגן ביעילות על התשתית הדיגיטלית שלהן.

בנוסף על פערי רגולציה, יש גם חוסר בפרוטוקולים סטנדרטיים לתגובה ושיקום לאחר אירועים, מה שיכול להשאיר ערים פגיעות במקרה של מתקפת סייבר. היעדר הנחיות ברורות כיצד להגיב לסוגים שונים של איומי סייבר יכול להוביל לעיכובים בזמני התגובה, להגדלת הנזקים, ולהוצאות התאוששות גבוהות יותר. פיתוח פרוטוקולים סטנדרטיים ותיעוד ברור של ניהול טכנולוגיות ערים חכמות ושל תגובה לאירועי סייבר הם קריטיים לשיפור הפרופיל של אבטחת הסייבר של עיריות.

חוסר הרגולציה והתיעוד יוצר גם אתגרים עבור עיריות מבחינת אחריות ומחויבות. במקרה של אירוע סייבר, עשוי להיות קשה לקבוע מי אחראי על הפריצה ומי צריך לשאת בעלויות ההתאוששות. חוסר ודאות כזה עלול להוביל למחלוקות בין עיריות, ספקי טכנולוגיה ובעלי עניין אחרים, ומסבך עוד יותר את תהליך ההתאוששות.

כדי להתמודד עם אתגרים אלו, על עיריות לעבוד עם גופים רגולטוריים לאומיים ובין-לאומיים כדי לפתח מסגרות מקיפות לניהול טכנולוגיות ערים חכמות ואבטחת סייבר. מסגרות אלו צריכות לכלול הנחיות ברורות לתגובה לאירועים, הגנה על נתונים וסטנדרטים של אבטחת סייבר, וכן פרוטוקולים לשיתוף פעולה בין עיריות, ספקי טכנולוגיה ובעלי עניין אחרים, בדומה לפרוטוקולים שקיימים עם פיקוד העורף במקרים של מלחמות, רעידות אדמה וכו'.

התמקדות בפרמטרים שניתן לשנות והתייחסות לשלוש תקופות זמן

במטרה לנסות ולגלות קשרים בין תקציבי אבטחת מידע, מדדים תקציביים אחרים ואירועי סייבר, המחקר בודק את הדינמיקה התקציבית העירונית בתל אביב ובהרצליה, את תהליך קבלת ההחלטות והשיקולים שנלקחו בעת חלוקת התקציב ואת פריסת סעיפי התקציב השונים בין מחלקות העירייה, וכן מנתח אירועי עבר. בעוד אנו בונים מטריצות קורלציה (מתאם) כדי לתאר בצורה חזותית את יחסי התקציב, נבחן גם ציר זמן של מתקפות סייבר לאורך 20 השנים האחרונות במהלך שלוש תקופות זמן עיקריות: טרום הטמעת טכנולוגיות העיר החכמה, במהלך הרצתן ובאזורים שבהם נוהלו כתוכנית פיילוט, ולאחר הטמעתן באופן מלא (במחלקות מסוימות).

תל אביב – האוכלוסייה גדלה, התקציב גדל; רק לא לאבטחת הסייבר

רוב סעיפי התקציב של העירייה, גדלים בהלימה לקצב גדילת האוכלוסייה בעיר, ראו למשל את תקציבי מערכות המידע, הביטחון והחינוך בתל אביב לאורך השנים האחרונות (ספרי התקציב של עיריית ת"א, 2015-2023). הגיוני שכאשר כמות האוכלוסייה גדלה גם התקציבים יגדלו, והנתונים של עיריית תל אביב אכן מראים קשרים חיוביים מובהקים בין התקציב הרגיל של חטיבת מערכות המידע והתקציב הרגיל הכללי ובין כמות האוכלוסייה בעיר. אולם עבור התקציב הרגיל של אבטחת המידע, המתאמים אינם מראים קשרים משמעותיים.

הממצא הזה מצביע על פער פוטנציאלי באסטרטגיית התקצוב של עיריית תל אביב, כאשר המיקוד בהרחבת התשתיות והשירותים הדיגיטליים אינו מתואם עם השקעה מקבילה באבטחת סייבר. ככל שהעיר ממשיכה לגדול ולאמץ יותר טכנולוגיות חכמות, כך חוסר האיזון הזה עלול לחשוף את תל אביב לסיכוני סייבר מוגברים, מה שמדגיש את הצורך בגישה מאוזנת יותר להקצאת תקציבים.

יתרה מזאת, היעדר הקורלציה המשמעותית בין גידול האוכלוסייה להקצאת תקציב אבטחת סייבר מראה שגישת התקצוב הנוכחית של תל אביב עשויה לא לקחת בחשבון באופן מספק את הסיכונים המוגברים לאבטחת סייבר הקשורים לאוכלוסייה גדלה ותשתית דיגיטלית מתרחבת. הפער הזה מדגיש את הצורך בגישה פרואקטיבית יותר לתקצוב, שבה השקעות באבטחת סייבר מותאמות בקנה מידה לגידול הדיגיטלי של העיר.

הגישה המאוזנת של הרצליה

בהרצליה קיים מתאם חיובי חזק בין גודל האוכלוסייה ותקציב חטיבת מערכות המידע והתקציב הרגיל, אך בשונה מתל אביב גם בין תקציב אבטחת המידע, אם כי נמוך במעט.

הגישה של הרצליה משקפת עמדה פרואקטיבית יותר באבטחת סייבר, שבה השקעות בתשתיות דיגיטליות מלוות בהוצאות מוגברות על אבטחת סייבר. התאמה זו מעידה על הכרה בטבע המשולב של שירותים דיגיטליים ואבטחת סייבר, ומדגישה את החשיבות של תכנון תקציב משולב לשיפור החוסן העירוני הכולל.

הניסיון של הרצליה מראה שגישה מתוכננת ומאוזנת היטב להקצאת תקציבים, שבה השקעות בטכנולוגיות ערים חכמות מותאמות על ידי גידול מקביל בהוצאות לאבטחת סייבר, יכולה לשפר את יכולת העיר לעמוד באיומי סייבר ולהתאושש מאירועי סייבר. אסטרטגיה זו לא רק עוזרת להגן על התשתית הדיגיטלית של העיר אלא גם בונה אמון ציבורי בבטיחות ובאמינות של שירותי ערים חכמות.

יותר תקציב לעיר החכמה, יותר תקציב להגנה

הרצליה מצטיינת לא רק בהלימה בין תקציבי המחלקות השונות בעירייה ותקציב אבטחת הסייבר, אלא גם כאשר משווים את תקציב העיר החכמה לתקציב אבטחת הסייבר נמצא מתאם חיובי, זאת על אף שלא נמצאה הלימה מובהקת בין תקציבי העיר החכמה לתקציבים אחרים בעירייה.

הגישה הפרואקטיבית שנקטה הרצליה מדגימה את החשיבות של ראיית אבטחת סייבר כחלק בלתי נפרד מפיתוח העיר החכמה. על ידי יישור ההשקעות באבטחת סייבר עם אלה בתשתית דיגיטלית, הרצליה יצרה סביבה עירונית בטוחה ועמידה יותר. גישה זו מספקת תובנות חשובות לערים אחרות המחפשות לפתח יוזמות ערים חכמות תוך צמצום סיכוני אבטחת הסייבר.

האסטרטגיה של הרצליה מדגישה גם את הצורך של עיריות לאמץ גישה הוליסטית יותר לתקצוב, שבה שיקולי אבטחת סייבר משולבים בכל ההיבטים של תכנון ופיתוח ערים חכמות. גישה זו מבטיחה שאבטחת הסייבר אינה מטופלת כדאגה נפרדת או משנית, אלא מוטמעת בכל היבט של התשתית הדיגיטלית של העיר.

כמות התושבים בעיר לא משפיעה, אבל אירוע סייבר כואב ודוח ביקורתי הם "Game changer"

בשנת 2021, לאחר שלוש שנים עם תקציב ללא שינוי, עיריית הרצליה הגדילה באופן דרמטי את תקציב אבטחת המידע הרגיל ב-25%. הסבר אפשרי לכך עשוי להיות מתקפת הסייבר הגדולה בדצמבר 2020, התקופה שבה נערכות ישיבות התקציב. בשנת 2022 חלה צמיחה משמעותית של התקציב הרגיל לאבטחת מידע ב-60%, כאשר לראשונה התקציב החריג הוקצה ברבע מהתקציב הרגיל. נראה כי תוצאות אלו נובעות מדוח מבקר המדינה שפורסם ב-2022 ועיקריו היו ידועים לעירייה כבר ב-2021 (State Comptroller of Israel, 2017, 2020, 2022).

גם בתל אביב, לאחר עשר שנים ללא התקפות גדולות, בשנת 2020 היה ניסיון לחדור למערכות העירוניות באמצעות התקפת "brute force" שכללה מידע סודי קריטי על המשתמשים העירוניים. העירייה החליטה להחליף את שרת האנטי וירוס ואת סינון המייל. ואכן, האירוע נתמך בעלייה החדה (יותר מפעמיים בהשוואה לשינוי בשנה הקודמת) בתקציב התוכנה והרישיונות ב-2021 (בשנה העוקבת).

בשנת 2021 גילו מנהלי אבטחת המידע מחשב נגוע בסוס טרויאני. במהלך תקופה זו החלה העירייה בפריסת מערכת חדשה – EDR. מתקפה זו אילצה את העירייה לבצע פרויקט דו-שנתי בפרק זמן של חודש ולהשתמש בתקציב חירום התומך בגידול החד בתקציב החריג לאבטחת מידע באותה השנה. אירוע זה ודוח מבקר המדינה שפורסם בשנת 2022, שעיקריו היו כאמור ידועים לעירייה כבר בשנת 2021, גרמו לעירייה להגדיל את תקציב אבטחת המידע הרגיל.

כל עירייה שונה

בעולם התוסס של פיתוח עירוני ואבטחת סייבר, תל אביב והרצליה בולטות בדוגמה שהן מציבות לניהול התקציבים והאמצעים להגנה מפני איומי סייבר. הסיפורים שלהן חושפים לקחים חשובים על איזון בין חדשנות דיגיטלית להגנה עמידה בפני איומי סייבר. איור 6א, 6ב ו-6ג משווים בין סעיפי התקציב השונים של תל אביב והרצליה.

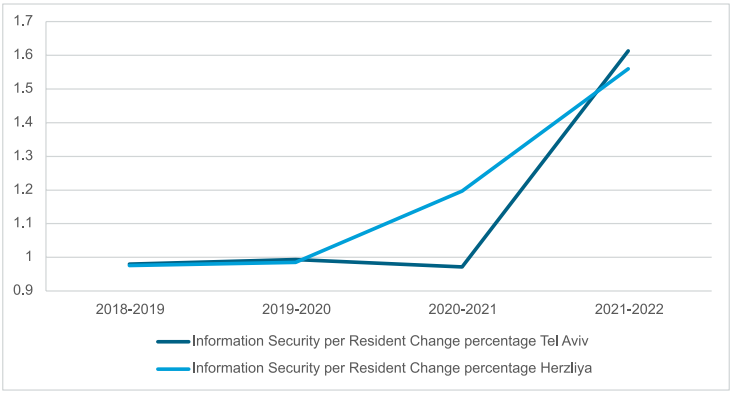
תל אביב, עם הדגש שלה על דיגיטציה מהירה ומודרניזציה, ראתה התקדמות רבה בשירותים ובתשתיות העירוניות. אולם גישה זו הביאה גם לחולשות חדשות מאחר שההשקעות של העיר בתחום הסייבר לא התקדמו בקצב הדיגיטלי שלה, כפי שניתן לראות באיור 6א אל מול איורים 6ב ו-6ג. חוסר באסטרטגיה פרואקטיבית בתחום הסייבר עלול להשאיר את תל אביב חשופה לאיומים גוברים ככל שהיא ממשיכה להרחיב את יוזמות העיר החכמה שלה.

תל אביב, הידועה בהתפתחות הדיגיטלית המהירה שלה, מרחיבה בצורה ניכרת את מחלקת המחשוב ומערכות המידע שלה. היא מבססת את עצמה כמפתחת "in-house" וההשקעה המרשימה שלה בכל תושב בתחום הטכנולוגיה מתבטאת היטב בתקציב. עם זאת, הסיפור מתהפך כשמדובר באבטחת סייבר. למרות כוח הדיגיטל של העיר, ההשקעות שלה בתקציב אבטחת סייבר לכל תושב מפגרות מאחור וחושפות תחום קריטי שדורש תשומת לב נוספת.

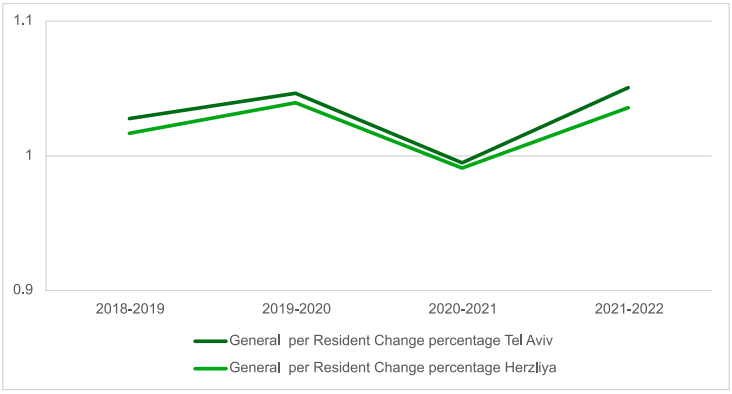
כפי שניתן לראות באיור 6א, בשנים האחרונות, התקציב של תל אביב לאבטחת סייבר חווה תנודות מסוימות. בשנת 2018 העיר חוותה מתקפת סייבר, והתגובה התקציבית לאחר מכן נראתה מתונה, ייתכן בשל ירידה נתפסת באיומים. אולם הסיפור השתנה בשנת 2022 כאשר בתקציב לאבטחת סייבר חלה עלייה משמעותית, כנראה כתגובה ישירה למתקפה חמורה בשנת 2021, שהראתה שהעיר שינתה את עמדתה בתחום האבטחה והגבירה את המאמצים להתמודד עם איומים עתידיים. באופן מעניין, אף שהחומרה של ההתקפות המוצלחות ירדה בשנת 2022, מה שמעיד על שיפורים באמצעי אבטחה, ההתנהגות של העיר המשיכה באופן זהה תוך מודעות עמוקה לנוף האיומים המשתנה.

לעומת זאת, הרצליה נקטה בגישה מאוזנת יותר, תוך שהיא נותנת עדיפות להשקעה בסייבר לצד פיתוח התשתיות הדיגיטליות. אסטרטגיה זו אפשרה להרצליה לבנות סביבה עירונית מאובטחת ועמידה יותר, תוך הפחתת הסיכוי למתקפות סייבר והפחתת ההשפעה שלהן כאשר הן מתרחשות. הניסיון של הרצליה מספק תובנות חשובות לערים אחרות שמבקשות לפתח יוזמות עיר חכמה ולנהל סיכוני סייבר בצורה אפקטיבית.

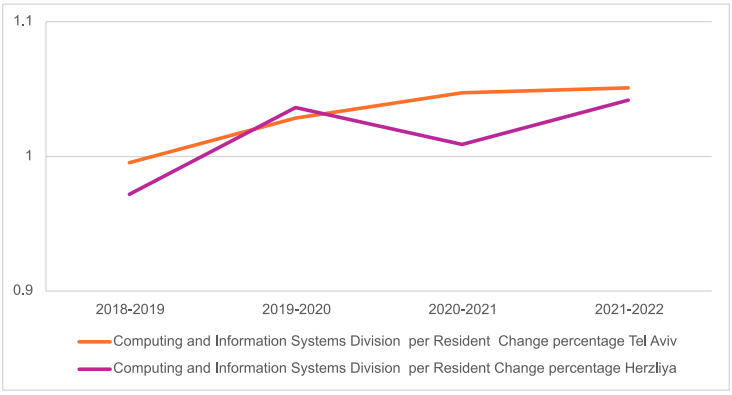
איור 6א: השוואת אחוז השינוי בסעיף התקציב של אבטחת מידע לתושב



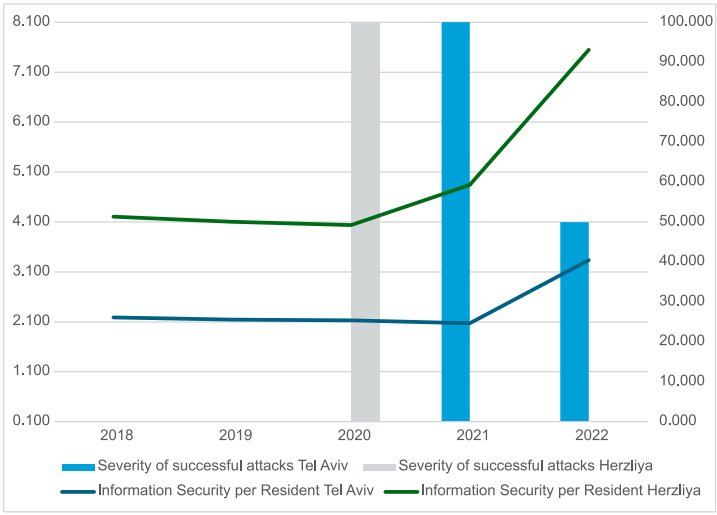
איור 6ב: השוואת אחוז השינוי בסעיף התקציבי הכללי לתושב



איור 6ג: השוואת אחוז השינוי בסעיף התקציב של חטיבת מערכות המידע לתושב



איור 7: השוואת הקצאות תקציב לתושב (ש"ח) לחומרת ההתקפות המוצלחות* (אחוז)



הגישה המקדימה הזו נראית משתלמת, שינויים בתקציבים נראו גם הם קשורים למתקפות סייבר, אך בגישה מעט שונה. תקציב אבטחת המידע עלה בצורה משמעותית בשנים האחרונות. בשנת 2021, לאחר שלוש שנים של תקציב יציב, הגדילה העירייה את התקציב הרגיל לאבטחת סייבר ב-25%, ככל הנראה בתגובה למתקפת סייבר גדולה בדצמבר 2020. בשנת 2022 גדל התקציב הרגיל לאבטחת סייבר ב-60%, והתקציב החריג לאבטחת סייבר הוקצה לראשונה ברבע מהתקציב הרגיל.

השפעת דוח מבקר המדינה שפורסם ב-2022 ניכרת גם בהרצליה, שם התקציב החריג לאבטחת סייבר עלה בצורה ניכרת לאחר הפרסום. שינויים אלו משקפים את ההשפעה של אירועים משמעותיים על תכנון התקציב וההשקעות בביטחון המידע. באיור 7 ניתן לראות את ההבדלים בתקציב אבטחת המידע לתושב אל מול חומרת ההתקפות השונות בשתי הערים, ואילו באיור 8 ניתן לראות מבט רחב יותר עם שאר סעיפי התקציב המרכזיים.

ואכן, הסיפורים השונים של תל אביב והרצליה מספקים תובנות חשובות לערים ולארגונים אחרים שמתמודדים עם אתגרים דומים. שתי הערים מדגישות את החשיבות שבהתאמת הקצאות התקציב לצרכים בתחום אבטחת הסייבר. הניסיון של תל אביב מדגיש את הצורך בהתאמות בזמן אמת בתגובה למתקפות, בעוד הגישה המאוזנת של הרצליה מדגימה את היתרונות של השקעה עקבית ומקדימה בתחום האבטחה. ניתן להגיד כי השקעה מאוזנת, הן ביזמות טכנולוגית והן בהגנת הסייבר, תהיה בעלת פוטנציאל גדול יותר למיצוב מהיר יותר של העיר כמתקדמת ועתידנית מאשר מרדף בלתי אחראי אחר טכנולוגיות חדשות ללא הגנה ראויה.

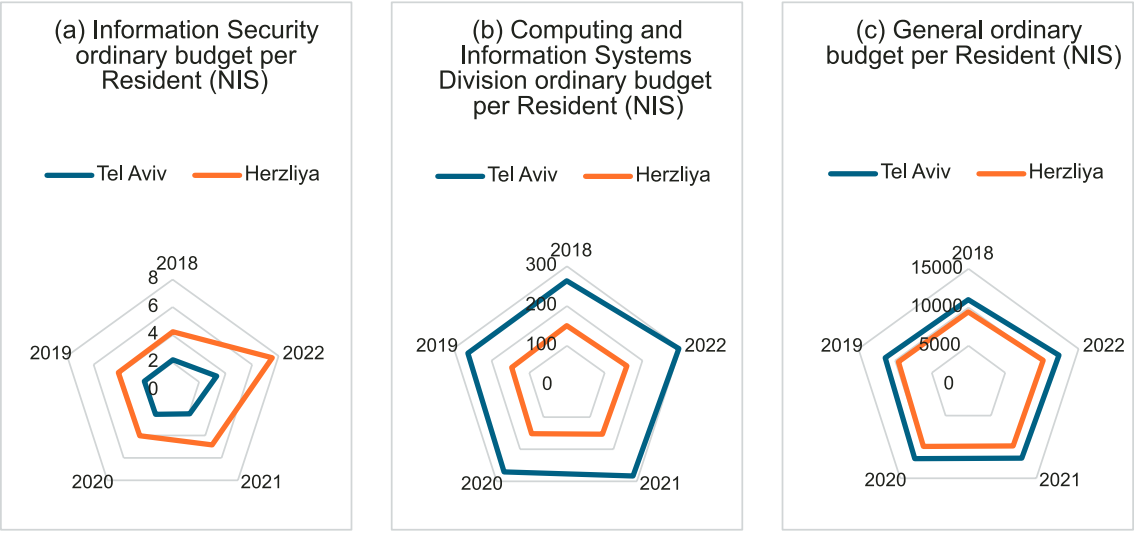
עבור מנהלות ומנהלי התעשייה, הסיפורים הללו חושפים ששיפור ניהול אבטחת הסייבר כולל לא רק השקעות משמעותיות בהתחלה, אלא גם סקירות והתאמות רגילות על בסיס איומים מתחדשים. באמצעות למידה מהמסעות של תל אביב והרצליה, ארגונים יכולים לנווט בצורה טובה יותר בנוף המורכב של אבטחת דיגיטלית וניהול תקציבים, ולוודא שהם נשארים עמידים מול איומי סייבר המשתנים.

תקציב זה טוב אבל זה לא מצוין

עלייה בתקציב היא חיונית לצורך התמודדות עם צורכי הסייבר, אך היא רק חלק ממתודולוגיה רחבה יותר. הערים תל אביב והרצליה מוכיחות כי השקעות כספיות בלבד אינן מספיקות לצורך מעטפת הגנת סייבר אפקטיבית. התמודדות עם איומי סייבר דורשת גישה מקיפה שכוללת גם תרבות ארגונית מתאימה, הכשרת עובדים ופרוטוקולי תגובה לאירועים.

* מידת חומרת מתקפת הסייבר הוערכה על פי מנהל אבטחת המידע בכל עירייה (מ. מיטלמן, תקשורת בינאישית, 3 ביולי 2022; א. זיו, תקשורת בינאישית, 6 ביולי 2022)

איור 8: הקצאת תקציב לתושב (ש"ח) לפי סעיפי תקציב שונים



מעבר להשקעה כספית, מתודולוגיה מקיפה לאבטחת סייבר כוללת גם טיפוח תרבות מתאימה בתוך הארגון, עדכון והכשרת עובדים על מיטב השיטות, והטמעה של אסטרטגיות תגובה אפקטיביות לאירועים. תל אביב והרצליה צריכות לשלב את המרכיבים הללו במסגרת האבטחה שלהן כדי לשפר את עמידותן בפני מתקפות עתידיות.

המנעד הלא מאוזן בהקצאות התקציב בין סעיפי התקציב השונים מדגיש גם את הצורך בגישה מאוזנת. בעוד שמימון מוגבר לצורך אבטחת סייבר הוא חיוני, הוא חייב להיות נתמך בהערכות סיכון מתמשכות ובצעדים פרואקטיביים להתמודדות עם חולשות סייבר. אסטרטגיית אבטחה מקיפה הכוללת משאבים כספיים, כלים תפעולים והיבטים תרבותיים, תהיה אפקטיבית יותר בהפחתת השפעת איומי סייבר והגברת האבטחה לאורך זמן.

טכנולוגיה מתקדמת מול רגולציה השייכת למאה הקודמת

בעידן הדיגיטלי של אבטחת מידע, רשויות מקומיות כמו תל אביב והרצליה מתמודדות עם אתגרים משמעותיים. הערים אומנם עשו צעדים חשובים בהתאמת התקציבים שלהן בתגובה לאיומי סייבר, אך נקודה חשובה שנשארה ברקע היא תפקידם של מסגרות רגולציה, או חוסר קיומן, בעיצוב האסטרטגיות שלהן לאבטחת מידע. היעדר חוקים מחייבים ומסודרים הוא בעיה יסודית שעלולה להשאיר ערים חשופות לאיומי סייבר ולסכן את יכולתן להגן על מידע רגיש ולשמור על תקינות התפעול.

בישראל, כמו במדינות רבות אחרות, הרגולציה על אבטחת מידע בקרב רשויות מקומיות היא לעיתים קרובות מעורפלת ומפוזרת. אין חוקים מקיפים ומחייבים המיועדים במיוחד לרשויות המקומיות שמחייבים עמידה בתקנים מדויקים. יש מדיניות ותקנות אבטחת מידע ברמה הלאומית, כמו אלה שמציב מערך הסייבר הלאומי, אך הן מתמקדות בעיקר בתשתיות לאומיות ובארגונים גדולים ולא מספקות הנחיות מפורטות לנוהלי אבטחת מידע ברמה העירונית.

כתוצאה מכך, הרשויות המקומיות פועלות בתחום רגולטורי אפור שבו אין חובה חוקית מפורשת המכתיבה צעדים מסוימים בתחום אבטחת המידע ברמה העירונית. היעדר קווים מנחים ברורים פירושו שערים כמו תל אביב והרצליה עשויות לנקוט גישות שונות לאבטחת מידע, לעיתים קרובות על פי ההתנסויות הישירות שלהן עם איומי סייבר במקום על פי מסגרת פרואקטיבית וסטנדרטית. ללא חוקי רגולציה ברורים, הדחיפות לפעול מתעוררת רק לאחר שמתרחש מקרה, מה שמוביל לצעדים תגובתיים ולא פרואקטיביים.

היעדר האכיפה הרגולטורית הביא לגישה התגובתית בתחום אבטחת המידע. הן תל אביב והן הרצליה הציגו זאת באמצעות תגובות תקציביות משמעותיות למתקפות סייבר חמורות. לדוגמה, העלייה הדרמטית בתקציב אבטחת המידע בתל אביב בשנת 2021 נבעה בעיקר בשל אירוע חדירת סוס טרויאני למערכי העירייה. בדומה לכך, בשנת 2021 חלה עלייה של 25% בתקציב אבטחת המידע בהרצליה אחרי מתקפת סייבר משמעותית. צעדים תגובתיים אלה מדגישים פגם קרדינלי: שיפוטי האבטחה מתבצעים לעיתים קרובות בתגובה להפרות בעבר במקום על פי ניהול סיכונים פרואקטיבי.

גישה תגובתית זו עלולה להיות מזיקה, שכן פעמים רבות היא מביאה לכך שהערים מטפלות רק באיומים המיידיים ביותר ולא מיישמות אסטרטגיות אבטחה מקיפות המכסות את כל הפגיעות הפוטנציאליות. היעדר הרגולציה המפורטת פירושו שאין פרוטוקולים סטנדרטיים עבור הערכות סיכונים סדירות, הכשרה לעובדים ותכנון תגובה לאירועים, הכלים המרכיבים את אבני היסוד של אבטחת המידע.

השלכות חוסר הרגולציה הן רחבות היקף, וללא סטנדרטים מחייבים הרשויות המקומיות עשויות להתמודד עם מספר בעיות:

1. **תנאי אבטחה לא אחידים** – היעדר מסגרת רגולטורית מאוחדת מביא לנוהלי אבטחת מידע לא אחידים בין רשויות מקומיות. הערים עשויות להיות מוכנות ברמות תגובה שונות, מה שמוביל להגנה לא אחידה מפני איומי סייבר.
2. **פגיעות מוגברת** – חוסר הרגולציה עלול להותיר את הרשויות המקומיות חשופות יותר למתקפות סייבר. ללא אמצעים מחייבים וביקורות סדירות, ייתכן שהערים יעמדו עם מערכות מיושנות, הגנות בלתי מספקות או עובדים לא מיומנים, מה שמגביר את פרופיל הסיכון שלהן.
3. **תגובת אירועים מאוחרת** – צעדים תגובתיים אומרים שהרשויות המקומיות עשויות להתמודד עם עיכובים בטיפול בפגיעות או בתגובה למתקפות. עיכוב כזה יכול להוביל לנזק גדול יותר, לעלויות התאוששות גבוהות יותר, ולתקופות ארוכות של השבתות שירותים.
4. **הקצאת משאבים לא יעילה** – בהיעדר רגולציה שמכתיבה כיצד יש להקצות תקציבי אבטחת מידע, ערים עשויות להשקיע משאבים בצורה לא יעילה. לדוגמה, כספים עשויים להיות מופנים בצורה לא פרופורציונלית לפרויקטים בולטים או לפתרונות זמניים במקום לבניית תשתית אבטחת מידע מקיפה וממושכת.
5. **אמון הציבור** – תקיפות וכישלונות רבים באבטחת מידע יכולים להפחית את האמון הציבורי בעיריות. האזרחים מצפים מהרשויות המקומיות להגן על המידע האישי שלהם ולוודא את תקינות השירותים הציבוריים. אמצעי אבטחת מידע לא מספקים, הנגרמים מחוסר רגולציה, עלולים להוביל לירידה באמון הציבור בעירייה.

כדי להתמודד עם בעיות אלו, חיוני לפתח ולהחיל רגולציה מקיפה לאבטחת מידע ברמה העירונית. רגולציה כזו צריכה לכלול:

1. **תקני אבטחה מחייבים** – החוקים צריכים לחייב אמצעי אבטחה מסוימים שיישמו הרשויות המקומיות, כולל הערכות סיכונים סדירות, עדכוני תוכנה וחומרה ותוכניות תגובה לאירועים.
2. **ביקורות והערכות סדירות** – נדרש לקבוע ביקורות סדירות כדי להבטיח עמידה בתקני אבטחת מידע. הערכות אלו יכולות לסייע בזיהוי חולשות פוטנציאליות ולהבטיח שהערים עוקבות אחרי שיטות העבודה הטובות ביותר.
3. **הכשרה והגברת המודעות לעובדים** – הרגולציה צריכה לכלול דרישות לתוכניות הכשרה סדירות כדי להבטיח שעובדי העירייה מודעים לאיומי הסייבר ומיומנים בשיטות העבודה הטובות ביותר לשם הגנה על מידע רגיש.
4. **פרוטוקולים לדיווח ותגובה לאירועים** – הנחיות ברורות צריכות להיות מוגדרות לדיווח ותגובה לאירועי סייבר, כולל קביעת לוחות זמנים לדיווח על מתקפות, בקרת נזקים ופרסום המידע הרלוונטי לגורמי מפתח.
5. **מימון והקצאת משאבים** – הרגולציה צריכה לספק הנחיות לרמות מימון מתאימות ולהקצאת משאבים עבור אבטחת מידע. זה מבטיח שהערים יעמדו ביכולת הכספית ליישם ולתחזק אמצעים יעילים לאבטחת מידע.
6. **שיתוף פעולה ומידע** – הרגולציה צריכה לעודד שיתוף פעולה בין רשויות מקומיות וסוכנויות אבטחת סייבר לאומיות (כמו השב"כ ומערך הסייבר הלאומי). שיתוף מידע על איומים, חולשות ושיטות עבודה מומלצות יכול לשפר את המאמצים הביטחוניים המשותפים.

החלת רגולציה מקיפה תעביר את הרשויות המקומיות מגישה תגובתית לגישה פרואקטיבית לאבטחת מידע. על ידי קביעת סטנדרטים וציפיות ברורות, הרשויות יכולות להתכונן טוב יותר לאיומים פוטנציאליים, להקצות משאבים ביעילות רבה יותר, ולשפר את עמידתן הכוללת לאבטחת מידע.

גישה פרואקטיבית כרוכה לא רק בתגובה לאיומים אלא גם בחיזוי ומניעת סיכונים פוטנציאליים לפני שהם הופכים לבעיות. זה כולל השקעה בטכנולוגיות מתקדמות, ביצוע הערכות פגיעות סדירות, וטיפוח תרבות של מודעות לאבטחת מידע בקרב עובדים ותושבים.

עולם שבו ערים נאלצות להתמודד כל הזמן עם אתגרי אבטחת מידע בלי שום הכוונה ברורה או תקנים מחייבים, הוא עולם שבו כל עיר נלחמת לבד ומבזבזת משאבים יקרים על פתרונות שהיו יכולים להיות יותר יעילים. זהו עולם של כאוס חמור, חוסר ארגון וחריגות בתקציב שיכולות להגיע למיליונים.

הדרישה לרגולציה צריכה לבוא דווקא מהעיריות

רגולציה מקומית מאפשרת יותר גמישות והתאמה מהירה לשינויים. הערים הן הגורם הקרוב ביותר לבעיות ולצרכים המשתנים של התושבים. כאשר הרגולציה מתקבלת מתוך העיר עצמה, היא יכולה להתעדכן באופן שוטף ומיידי בהתאם לשינויים באיומים ובטכנולוגיות. לדוגמה, אם עיר נתקלת בסוג חדש של מתקפת סייבר, הרגולציה המקומית יכולה לעדכן את ההנחיות והתקנים במהירות, מה שמסייע לעיר להישאר צעד אחד קדימה בהגנה על המידע שלה.

נוסף על כך, כאשר הערים לוקחות יוזמה בתחום הרגולציה הן גם יכולות לנצל את הידע המקומי והניסיון המיוחד שיש להן בתחום האבטחה. צוותים מקומיים שעובדים ישירות מול האתגרים העירוניים, מבינים את המורכבויות והצרכים בצורה עמוקה יותר מאשר גופים רגולטוריים כלליים. הם יכולים ליצור פתרונות שמתאימים למציאות המקומית ולא לנסות להפעיל שיטות שעובדות בצורה טובה בערים אחרות אך אינן מתאימות להן.

עוד יתרון חשוב של רגולציה שמנוהלת מתוך הערים הוא היכולת לחסוך בעלויות. כאשר הערים יוזמות רגולציה הן יכולות לעצב את התקנים כך שיתאימו לתקציב המקומי וימנעו הוצאות מיותרות. זה עוזר למנוע בזבוז של משאבים על דרישות שיכולות להיות יקרות מדי או שאינן נדרשות במציאות המקומית. על ידי התאמת הרגולציה לצרכים וליכולות התקציביות, הערים יכולות להבטיח שהן מקבלות תמורה מקסימלית להשקעתן בתחום האבטחה.

לבסוף, כאשר הערים יוזמות את הרגולציה הן מקבלות הזדמנות להנחות את השיח הציבורי ולהשפיע על המדיניות הכללית בתחום האבטחה. זה מעניק להן כוח והשפעה בקביעת סטנדרטים שיכולים לשרת ערים נוספות ולהוות מודל לחיקוי. כך, הערים לא רק מעמידות את האתגרים והצרכים שלהן על סדר היום, אלא גם משפיעות על שינוי מדיניות ברמה רחבה יותר.

במבט כולל, רגולציה שמגיעה מתוך הערים מאפשרת להן להיות מותאמות יותר לצרכים ולאתגרים המקומיים, לחסוך בעלויות ולהגיב במהירות לשינויים. זה לא רק מסייע לערים לנהל את האתגרים בתחום האבטחה בצורה יותר יעילה, אלא גם מאפשר להן להנחות את השיח ולתרום ליצירת סטנדרטים שמועילים לכלל הערים. כאשר הערים לוקחות את המושכות לידיים, הן יוצרות סביבה בטוחה ומסודרת יותר, ומפנות את הדרך לעתיד יציב ומוגן.

יישור קו רגולטורי הוא דבר טוב, אך עלול ליצור פער בין עיריות עשירות ועניות

ככל שערים חכמות משלבות טכנולוגיות IoT מתקדמות יותר, כך הצורך ברגולציה חזקה בתחום אבטחת המידע הופך להיות קריטי. עם זאת, אחד האתגרים הגדולים נעוץ באופי המקומי של רגולציה זו. ערים גדולות ועשירות יותר, בעלות תקציבים נרחבים וצוותי מחשוב חזקים, מסוגלות להקים מחלקות ייעודיות לאבטחת מידע ואף לשכור מנהל אבטחת מידע (CISO) מנוסה. לעומת זאת, ערים קטנות או עניות יותר, שאינן מחזיקות צוותי מחשוב חזקים ולעיתים אף מסתמכות על מיקור חוץ, עומדות בפני קושי משמעותי בפיתוח רגולציה יעילה ובניהול אבטחת המידע שלהן. אפשר להשוות בין עיריית תל אביב ועיריית הרצליה, שתיהן עיריות עשירות להפליא, אך נבדלות בגודל האוכלוסייה. תל אביב מנהלת מחלקה פנימית שלמה שתפקידה אבטחת מידע, ואילו הרצליה מעסיקה צוות אבטחת מידע קטן.

עיריות קטנות שנכנסות לפרויקטים של IoT בתמיכה חיצונית, ניצבות בפני שאלה מורכבת: האם מצופה מהן לא רק ליישם את הפרויקטים אלא גם לפתח גוף ידע פנימי שיהווה רגולטור מקומי? מצב זה מעלה סיכון לפערי אבטחה משמעותיים בין עיריות עשירות לעיריות פחות מבוססות. בעוד שהראשונות

עשויות לפתח מערכות מתקדמות ולהגיב במהירות לאיומים, האחרונות עלולות להישאר מאחור, מה שיוביל לפגיעות משמעותית בתשתיות שלהן.

גוף ארצי, שותפויות ציבוריות-פרטיות, תמריצים ממשלתיים ורגולציה דינמית

הפערים שעלולים להיווצר בין ערים עשירות לערים עניות הם מרכיב קריטי בבניית הרגולציה ואין להתעלם מהם. יש לנסות למצוא פתרונות שמגשרים על פערים אלו ולוקחים בחשבון את הדיפרנציאציה בין הערים.

דוגמה לפתרונות אפשריים:

1. **הקמת גוף ארצי תומך** – יצירת גוף ארצי שיספק תמיכה רגולטורית וטכנית לעיריות קטנות. גוף כזה יכול לנסח סטנדרטים אחידים, להציע שירותי אבטחת מידע במודל משותף (Shared Services) ולספק ייעוץ וליווי עירוני מתמשך.
2. **שותפויות ציבוריות-פרטיות (PPP)–** עידוד שותפויות עם חברות טכנולוגיה לצורך הקניית ידע, תחזוקה שוטפת, וניהול אבטחת מידע בעלות מופחתת עבור עיריות בעלות משאבים מוגבלים.
3. **תמריצים ממשלתיים** – מימון ייעודי או סובסידיות לעיריות קטנות לצורך העסקת מומחים לאבטחת מידע או לשדרוג התשתיות שלהן, תוך הבטחת מינימום תקני אבטחה.
4. **שימוש ברגולציה מותאמת קונטקסט** – פיתוח מסגרות רגולטוריות הדרגתיות המתחשבות בגודל העיר ובמשאביה, כך שעיריות קטנות יוכלו לעמוד בדרישות ללא עומס יתר על התקציב. יש לאזן בין ההתחשבות במחויבויות העירייה לבין הפגיעה הפוטנציאלית בביטחון המידע ופרטיות התושבים.

סיכום

במאמר זה בחנו את הקצאת התקציבים העירוניים, בדגש על אבטחת סייבר, על רקע ההתקדמות הטכנולוגית המהירה והדיגיטציה הגוברת של מערכות עירוניות. תוך התמקדות בתל אביב והרצליה כמקרי מבחן, המחקר בוחן כיצד החלטות תקציביות משפיעות על מוכנות אבטחת סייבר, אסטרטגיות תגובה וחוסן עירוני כללי. על ידי בחינת מתאמים בין תקציבי אבטחת מידע ומשתנים כמו גודל אוכלוסייה, הוצאות מוניציפליות כלליות ויוזמות עיר חכמה, המחקר שופך אור על יחסי הגומלין המורכבים השולטים בהקצאות כספיות בממשל עירוני מודרני.

הממצאים מדגישים מגמות מגוונות בין שתי הערים, וחושפים כי גודל האוכלוסייה אינו מותאם באופן עקבי עם הקצאת תקציב אבטחת מידע, תוך שימת דגש על השפעתם של גורמים דמוגרפיים והקשרים רחבים יותר. עוד חושף המאמר כי יש קשרים מגוונים בין תקציבי עירייה כלליים ותקציב אבטחת המידע בתל אביב ובהרצליה, מה שמצביע על הצורך באסטרטגיות דינמיות המותאמות לנסיבות הייחודיות של כל עיר.

מאמר זה מציע תובנות שיש להתחשב בהן בעת בניית תקציבים עירוניים שנתיים. ממצאי המחקר מציעים השלכות מעשיות למנהלי העירייה ולעוסקים באבטחת סייבר, ומאפשרים להם לייעל החלטות פיננסיות, לצפות את ההשפעות של אירועי סייבר על התכנון התקציבי, ולאמץ גישות מותאמות המתייחסות לצורכי אבטחת סייבר ספציפיים במסגרת שיקולים תקציביים רחבים יותר.

ד"ר שחר רייכמן sr@tauex.tau.ac.il
ד"ר יעקב מנדל jacob4x4@gmail.com
יואב זיו yoavziv1@mail.tau.ac.il

רשימת מקורות

Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. *IEEE Access*, *8*, 228922–228941.

Bogdoll, D., Matalla, P., Füllner, C., Raack, C., Li, S., Käfer, T., ... & Bonk, R. (2021, September). Kiglis: smart networks for smart cities. In *2021 IEEE International Smart Cities Conference (ISC2)* (pp. 1–4). IEEE.

Cerrudo, C., & Spaniel, D. (2015). Keeping smart cities smart: preempting emerging cyber attacks in US cities. *Institute for Critical Infrastructure Technology*.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491–497.

Feachem, R. G., Graham, W. J., & Timaeus, I. M. (1989). Identifying health problems and health research priorities in developing countries. *The Journal of tropical medicine and hygiene*, *92*(3), 133–191.

Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia computer science*, *52*, 1089–1094.

ITC. (2022). ITC – Spend less time on the road.

Khan, F., Kumar, R. L., Kadry, S., Nam, Y., & Meqdad, M. N. (2021). Cyber physical systems: A smart city perspective. *International Journal of Electrical and Computer Engineering*, *11*(4), 3609.

Kuddus, M. A., Tynan, E., & McBryde, E. (2020). Urbanization: a problem for the rich and the poor?. *Public health reviews*, *41*, 1–4.

Kusumawati, D., Setiawan, D., & Suryanegara, M. (2017, October). Spectrum requirement for IoT services: A case of Jakarta smart city. In *2017 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)* (pp. 21–25). IEEE.

McMichael, A. J. (2000). The urban environment and health in a world of increasing globalization: issues for developing countries. *Bulletin of the world Health Organization*, *78*, 1117–1126.

Mondschein, J., Clark-Ginsberg, A., & Kuehn, A. (2020, December). Smart Cities as Large Technological Systems: Collective Action Problems as Organizational Barriers to Urban Digital Transformation. In *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*.

Ricciardi, F., & Za, S. (2014). Smart city research as an interdisciplinary crossroads: a challenge for management and organization studies. In *From information to smart society: Environment, politics and economics* (pp. 163–171). Cham: Springer International Publishing.

State Comptroller of Israel. (2017). The Local Government Audit Report for 2017.

State Comptroller of Israel. (2020). The Local Government Audit Report for 2020.

State Comptroller of Israel. (2022). The Local Government Audit Report for 2022.

Transforma Insights. (2020). Global IoT Forecast Insight Report 2020.

Transforma Insights. (2022). Global IoT Forecast Report, 2021–2030.

United Nations, Department of Economic and Social Affairs, Population Division. (2018). World urbanization prospects: The 2018 revision.

Washburn, D., Sindhu, U., Balaouras, S., Dines, R. A., Hayes, N., & Nelson, L. E. (2009). Helping CIOs understand "smart city" initiatives. *Growth*, *17*(2), 1–17.