סקר אבטחת מידע

איתור וחשיפת זליגות מידע באמצעות רשתות אלחוטיות

1. הקדמה

רשת תקשורת המחשבים הפנימית של העירייה מכילה מידע רגיש אשר נמצא בשימוש המחלקות השונות הכולל בין היתר מידע פרטני על אזרחים, תשלומים, מבנים ועוד. מטרת הסקר הינה להבטיח ולוודא את שמירת סודיותו,אמינותו וזמינותו של המידע ברשת הארגונית מניסיון של תוקף פוטנציאלי להתחבר לרשת הארגון הפנימית באמצעות התקן שידור רשת אלחוטי.

2. שיטת עבודה

שיטת העבודה לביצוע הבדיקה כללה סיור רגלי בין מבני העירייה בליווי נציג ממחלקת המחשב ומדידת עוצמת שידורים של רשתות אלחוטיות. המדידה בוצעה בעזרת מחשב נייד, כרטיס רשת אלחוטי ותוכנה ייעודית למטרה זו.

3. ממצאים וחשיפות

להלן מוצגים הממצאים והחשיפות אשר תועדו בעת ביצוע הבדיקות באתרי העירייה הבאים:

3.1 מחשבים ניידים עם כרטיסי רשת אלחוטיים

רקע:

במהלך הסיור הרגלי במבני העירייה נסרקו תדרי אלחוט ועוצמות שידור של רכיבי תקשורת אלחוטית הנמצאים בחצרות העירייה.

ממצא:

במהלך הבדיקה נסקר בניין מספר 7 של העירייה, ונמצא כי ישנו שידור אלחוטי חזק עם מזהה רשת: Hpsetup וללא כל הצפנת רשת או הגנת סיסמא (open). מזהה רשת זה מסגיר כי הרכיב המשדר הינו מתוצרת חברת HP. עוצמת שידור גבוה במיוחד נמדדה באזור הכניסה לחדרו של מבקר העירייה. בחדרו נמצא מחשב נייד מתוצרת חברת HP שנמצא בתחנת עגינה המחוברת לרשת העירייה בצורה קווית וכרטיס הרשת האלחוטי הופעל עם הגדרות שיתוף אינטרנט וקבצים.

השלכה/סיכון:

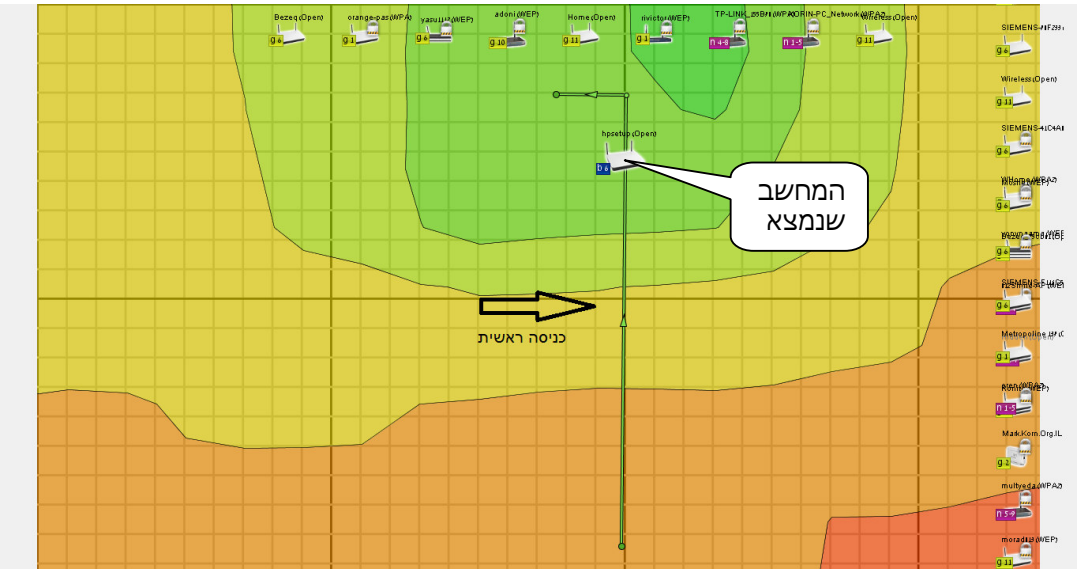
תצורה זו של כרטיס הרשת האלחוטי מאפשרת חיבור של גורם זר/זדוני לרשת העירייה וגישה למערכותיה והמידע הנמצא בהן ובנוסף, גישה לקבצים הנמצאים על המחשב עצמו ללא שום צורך בסיסמא או הזדהות וכך יוכל לפגוע בזמינות, אמינות וסודיות הנתונים בעירייה.
ניתן לראות בצילומי המסך להלן, כי אות השידור האלחוטי המשודר מהמחשב הנייד חזק דיו ובטווח הקליטה נמצאים בנייני מגורים.

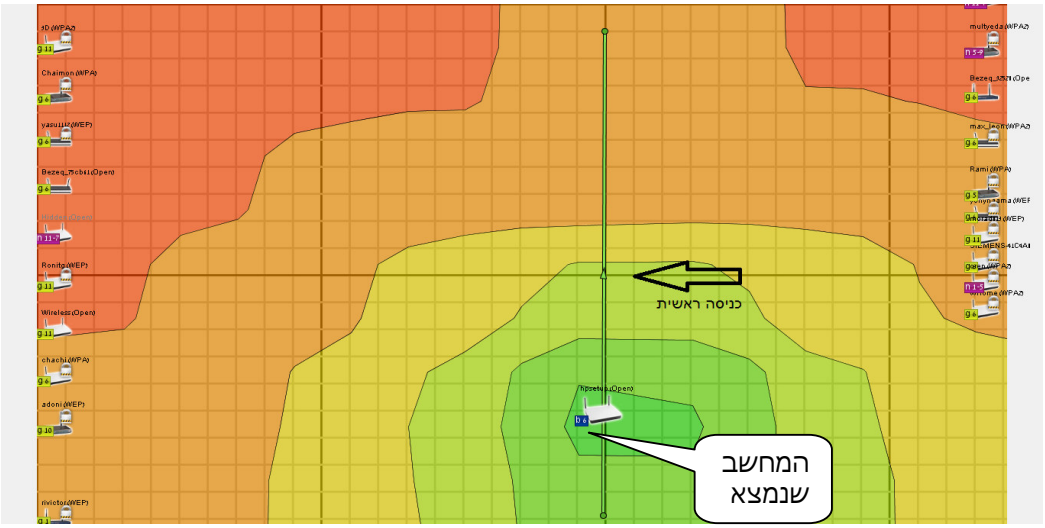
המלצה:

יש לוודא כי בכל עת בה מחוברים המחשבים הניידים בחיבור קווי לרשת העירייה הפנימית, יועבר כרטיס הרשת האלחוטי למצב כבוי (Disable) ללא אפשרות של משתמש הקצה להפעילו.

בצילומי המסך הבאים ניתן לראות את מסלול המדידה בתוך המבנה, טווח הכיסוי של אות השידור האלחוטי מהמחשב הנייד ואת המחשב הנייד עצמו.

- בצילום מסך זה ניתן לראות את מסלול ההליכה במבנה מס׳ 7, בקומת הכניסה (מסומן בחץ ירוק על גבי התמונה). בשולי התמונה ניתן להבחין במספר רב של רשתות אלחוטיות שנמצאות בטווח הבניין.






Microsoft
Coral

3.2 נתב רשת אלחוטי המחובר לרשת העירייה

רקע:

במהלך הסיור הרגלי במבני העירייה נסרקו תדרי אלחוט ועוצמות שידור של רכיבי תקשורת אלחוטית הנמצאים במבני העירייה השונים.

ממצא:

במהלך הבדיקה נסקר בניין מחלקת הרווחה - כרמל, כאשר נסרקה הקומה השנייה במבנה, נמצא כי ישנו אות שידור אלחוטי חזק המגיע מתוך המבנה ונמצא במסלול הסריקה עם מזהה רשת מוסתר (Hidden), ובעל הצפנה מסוג WEP. לאחר בדיקה נתגלה נתב רשת אלחוטי המחובר לארון התקשורת של רשת העירייה.

השלכה/סיכון:

חיבור מסוג זה מהווה חשיפה חמורה לרשת הארגונית של העירייה מכיוון שתוקף פוטנציאלי יוכל לעקוף בקלות את ההצפנה מסוג WEP ולקבל גישה לרשת הפנימית של העירייה ובכך לפגוע בזמינות, אמינות ושלמות הנתונים בעירייה.

המלצה:

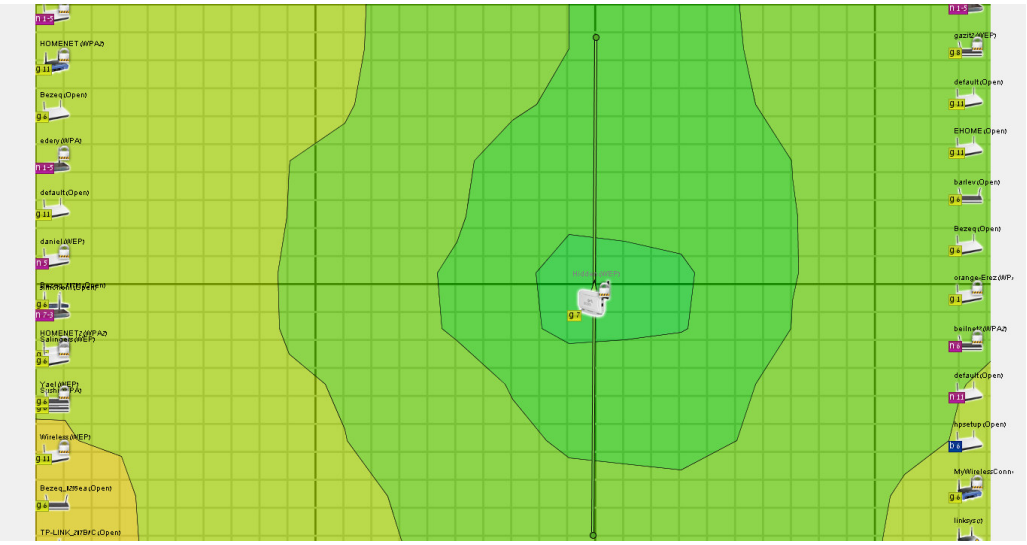
יש לשקול הטמעת מערכת ניטור אוטומטית לבקרת גישה לרשת (NAC). מערכת זו מזהה התקנים לגיטימיים המחוברים לרשת ויכולה לדווח ולחסום בכל מקרה של התקן זר אשר חובר לרשת.

יש להתאים בין מבואת המתג לכרטיסי הרשת של מחשבי העירייה (יש לשקול לעשות שימוש בטכנולוגית 802.1X ובתעודות דיגיטליות), לנתק את המבואות שאינן בשימוש.

יש לוודא שארונות התקשורת נעולים בכל זמן כך שאין גישה לכל אדם לבצע חיבור פיזי או שינוי הגדרות לציוד התקשורת.

מומלץ לחזור על הבדיקה ולסרוק את מבני העירייה אחת לשנה על מנת לוודא שלא בוצעו חיבורים בלתי מורשים של אמצעי שידור רשת אלחוטיים לרשת הארגונית.

בצילומי המסך הבאים ניתן לראות את מסלול המדידה בתוך המבנה בקומה השנייה, טווח הכיסוי של אות השידור האלחוטי מהנתב בארון התקשורת הפתוח ואת הנתב עצמו.




3Com

3.3 גישה חופשית לנתב רשת אלחוטי בחדר ישיבות במבנה "החאן"

רקע:

במהלך הסיור הרגלי במבני העירייה נסרקו תדרי אלחוט ועוצמות שידור של רכיבי תקשורת אלחוטית הנמצאים בחצרות העירייה.

ממצא:

בחדר הישיבות שבמבנה "החאן" נמדדה עוצמת שידור גבוה ממודם-נתב רשת אלחוטי בעל מזהה רשת ChanKsaba ללא הצפנת רשת והגנת סיסמא (Open) המשמש לחיבור אינטרנט בעיתות דיונים ואסיפות.

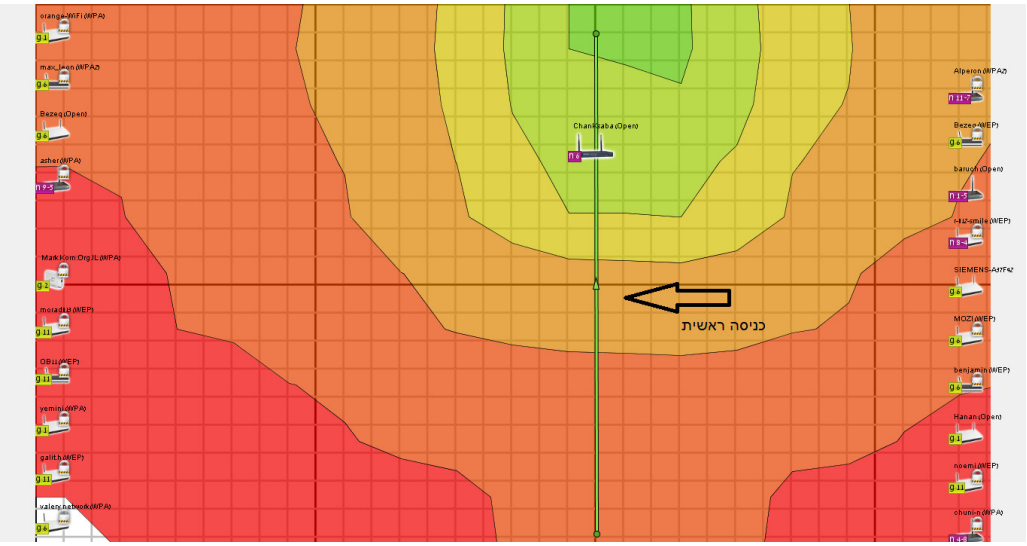
השלכה/סיכון:

החוסר בהצפנת רשת וסיסמא הזדהות מאפשר לכל אחד להתחבר ולהיות חלק מהרשת אותה מקיים הנתב, כמו כן, בטווח הכיסוי השידור האלחוטי נמצאים בנייני מגורים ואזורים ציבוריים מהם ניתן להתחבר לרשת באין מפריע.
כאשר מתקיימים דיונים והנוכחים מתחברים ממחשבים ניידים או מכשירי טלפון חכמים לרשת האינטרנט האלחוטית בחדר הישיבות, באפשרותו של תוקף פוטנציאלי להוציא לפועל התקפות שונות הכוללות התחזות (Phishing), יירוט תעבורת אימייל, שליפת סיסמאות גישה לאתרים, קבלת גישה לקבצים, האזנה והקלטת התעבורה הכולל מידע חסוי ורגיש של כלל משתמשי הרשת.

המלצה:

בהגדרות הנתב יש להפעיל הצפנת רשת WPA2 , ולהזין סיסמא בת 8-14 תווים.
באופן הזה יוכלו להתחבר אל הרשת מורשי גישה ותמנע גישת זרים.
יש להפעיל מנגנון סינון גישה על פי כתובת פיזית (MAC) ולהזין לנתב אך ורק כתובות של מורשי הגישה לרשת.

בצילומי המסך הבאים ניתן לראות את מסלול המדידה בתוך המבנה, טווח הכיסוי של אות השידור האלחוטי מהנתב ואת הנתב עצמו.


כניסה ראשית

3.4 חיבור רשת העירייה לרשתות חיצוניות

רקע:

במהלך הבדיקה נתגלו רשתות אלחוטיות רבות במתחם ההיקפי אשר מבני העירייה נמצאים בטווח הכיסוי שלהן, חלקן מוגנות בסיסמא וחלקן האחר לא, כך שניתן להתחבר אליהן מתוך מתחם מבני העירייה ללא קושי.

השלכה/סיכון:

באמצעות חיבור כרטיס רשת אלחוטי בממשק USB לכל אחת מתחנות העבודה ברשת הארגון הפנימית, ניתן להתחבר ו/או לגשר (Bridge) אל כל אחת מהרשתות האלחוטיות החיצוניות. התחברות לרשת חיצונית מתחנת עבודה ברשת הארגונית תאפשר דליפת מידע על ידי העברת מידע מהרשת הפנימית באמצעות רשת חיצונית לכל מקור. גישור הרשת הפנימית לרשת חיצונית יאפשר העברת מידע פנימי לרשת חיצונית ולמימוש התקפות מסוגים שונים לרבות התחזות ומניעת שירות (DoS).

כמו כן, נמצא כי עובדי העירייה מתחברים לרשתות אלחוטיות שאינן מוכרות ממכשירי טלפון חכמים לבדיקת דואר אלקטרוני או גלישה באינטרנט.

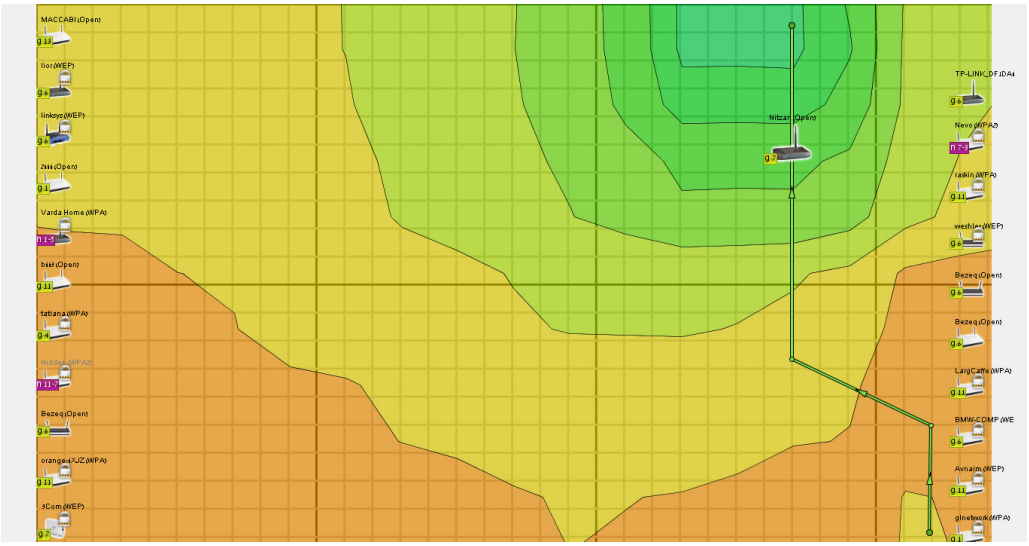
המלצה:

יש למנוע חיבור והתקנה של כרטיסי רשת אלחוטיים על ידי צמצום הרשאות משתמשים ומניעת האפשרות להתקנת דרייברים במדיניות קבוצות ארגונית (GPO).

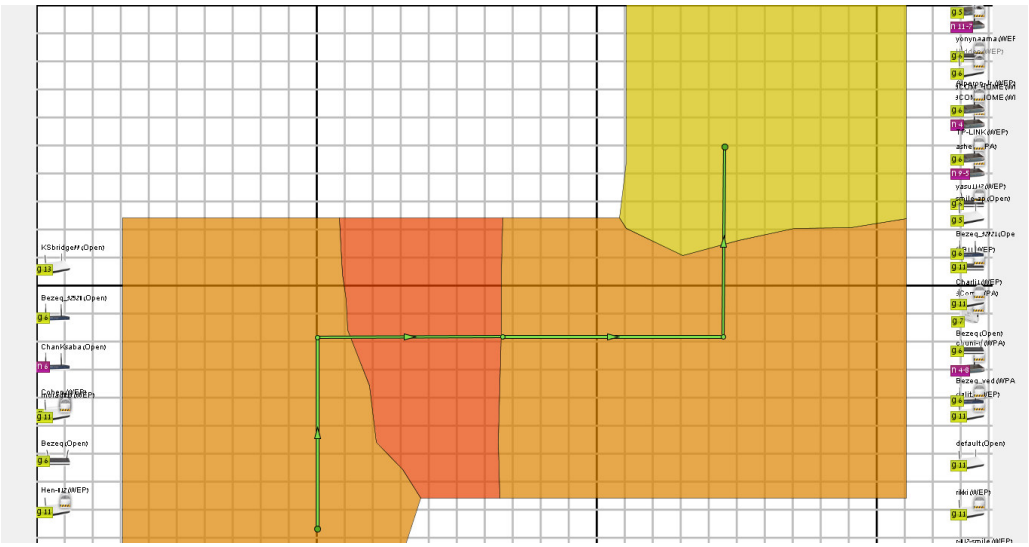
במחשבים בהם מוגדר כרטיס רשת אלחוטי, יש להגדיר רשימת רשתות מותרות בשימוש ולחסום את גישת המשתמש מלשנות רשימה זו. ראה הרחבה לסעיף זה בהמלצה לממצא 1.

בצילומי המסך הבאים ניתן לראות רשתות אלחוטיות חיצוניות אשר מבני העירייה נמצאים בטווח כיסוי אפשרי למימוש החשיפה:

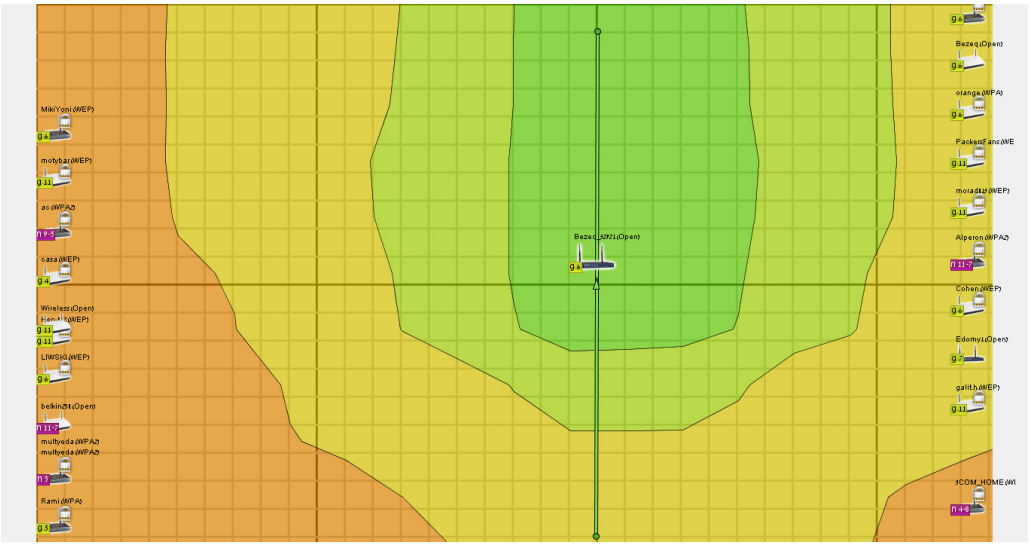
- <u>מבנה תהיל״ה - מרכז המחשוב של העירייה</u>



- מבנה מפעל המים



- מחלקת גבייה - קומה ב'



4. סיכום

רמת האבטחה המיושמת בתשתית התקשורת ובתחנות הקצה בעירייה מאפשרת לגורם זר/זדוני להתחבר בנקל לרשת העירייה ובכך להשפיע על זמינות, אמינות ושלמות הנתונים במערכות המידע בעירייה.

אנו ממליצים לבחון בחיוב הטמעת מערכת ניטור אוטומטית לבקרת גישה לרשת (NAC) ובמקביל, לעדכן וליישם מדיניות קבוצות ארגונית (GPO) על מנת לצמצם חשיפות אפשריות על ידי הגבלת הרשאות המשתמשים וצמצום גישה למשאבי מערכת.

מנהל האגף למחשוב ומערכות מידע מסר לביקורת כי הבקשה לרכישת מערכת ניטור לבקרת גישה לרשת נכללה בהצעת התקציב לשנת 2012.

נספח א' - ביאור מושגים טכניים

- **WiFi**- הוא השם העממי למספר תקנים לציוד רשת אלחוטית במרחב מקומי (Wireless LAN) המבוססים על תקן IEEE 802.11.
  תקנים אלה מאפשרים פריסת רשת תקשורת בגלי רדיו שבה משודרות חבילות נתוני IP בין הצרכנים השונים, למרחקים של כמה עשרות או מאות מטרים. מקור השם Wi-Fi הוא בקיצור הביטוי ,Wireless Fidelity על משקל הכינוי Hi-Fi שניתן בעבר למערכות סטריאו.
- **WEP** (**Wired Equivalent Privacy**) הוא אלגוריתם אבטחה לרשתות נתונים אלחוטיות העומדות בתקן IEEE 802.11. מטרת פיתוחו של האלגוריתם הייתה, לספק פרוטוקול אבטחה לרשתות אלחוטיות באותה רמת אבטחה שסופקה לרשתות נתונים קוויות. תפיסת הפעולה מתבססת על הצפנת הנתונים לצורך העברתם בצורה מאובטחת.
  כשלי אבטחה שנתגלו בפרוטוקול הקריפטוגרפי הובילו בהמשך לפיתוח ה-WPA.
- **WPA\WPA2** (**Wi-Fi Protected Access**) הם שני פרוטוקולי אבטחה שפותחו על ידי התאחדות ה WiFi במטרה לאבטח רשתות אלחוטיות. אלו פותחו בעקבות פריצות חמורות שנמצאו על ידי מומחים במערכת הקודמת WEP.
- **NAC** (**Network Access Control**) הינה מערכת המאפשרת לארגונים לעקוב אחר גישת תחנות קצה וגורמים שונים ברשת, פעילותם, ומצב אבטחתם באופן מתמשך, הן בתהליך התקשרותם לרשת והן לאחריה.
- **כתובת MAC** (**Media Access Control address**) היא מזהה ייחודי המוטבע על כל רכיב תקשורת לתקשורת נתונים בעת הייצור. כתובת ה- MAC מוטבעת בדרך כלל בכרטיס הרשת של המחשב ו/או במודם.

- **מדיניות קבוצתית (Group Policy ,GPO)** היא תכונה של מערכות הפעלה השייכות למשפחת .NT 5.0 . מדיניות זו מאפשרת לנהל קבוצות של מחשבים על פי מדיניות הנקבעת בידי מנהל המחשוב ומוחלת על המחשבים המנוהלים. המדיניות הנאכפת על המחשב קובעת הגבלות ואפשרויות שימוש במחשב (לדוגמה: מניעת שינוי השעה בשעון, הגבלה של סמלים בלוח הבקרה, הגבלות על שינוי תיקיות במחשב).