גרסת הסייבר החדשה- התקפות על הרשויות מוניציפליות

סכנה: אחרי גל התקפות המיילים והדלפות תמונות אישיות של אנשים ידועים, חברות הטכנולוגיה מעידות על מתקפת סייבר חדשה שעשויה לפגוע ברשויות המוניציפליות שמחזיקות לא מעט מידע מסווג אודות התושבים

המודעות לתקיפות סייבר במרחב האישי הולכת וגדלה כדוגמת פריצות למיילים אישיים של אנשים, פריצה למכשירי הסלולר והדלפת תמונות אישיות. במקביל למרחב האישי, מתקפות יכולת להתרחש גם במרחב הלאומי כמו חדירה למידע מסווג בצה"ל, תשתיות לאומיות וכ"ו. מלבד זאת, יש מקום אחד שחשוף למתקפות כיום, אבל לא רבים מודעים לסכנה הקיימת וזו מתקפת הסייבר על הרשויות המוניציפליות שמחזיקות לא מעט מידע מסווג אודות התושבים. מאגרי הרשות הנתונים של הרשות מכילים מידע רגיש מאוד של התושבים כדוגמת פרטים אישיים, תוכניות פנימיות ותקציבים, מידע אישי של אמצעי סליקה, החלטות פנימיות לפני פרסום, דוחות חנייה ,דוחות עסקים ועוד.

אריה טרבלסי מנכ"ל חברת סופר קום המתמחה במתן פתרונות זיהוי, אבטחה ומעקב מסביר: "המעבר לטכנולוגיות חדשות מחייב את הרשויות המקומיות ליישר קו אל מול האתגרים החדשים לאבטחת הנתונים, שכן הרשויות המקומיות עברו מהפלטפורמות המסורתיות למובייל. מעבר זה, הרחיב את קשת האיומים ואפשרויות החדירה איתם מתמודדת הרשות המקומית. היום, ממכשיר סלולארי אחד ניתן להפיל מערכות מידע של רשות שלמה. פריצה לאתר אינטרנט של העירייה בו ניתן לבצע פעולות רגישות כגון תשלומים; פגיעה במערכות קריטיות של הרשות; פריצה דרך Unsecured Wi-Fi לשרת הדואר של עירייה לקבלת גישה למידע פנימי והפצת וירוסים; גלישה לאתרים שנגועים בוירוסים; פריצה דרך שרתיי העיריה; פריצה דרך הפקס של העירייה; פריצה ע"י שליחת דואר אלקטרוני שבפתיחתו מאפשר הכנסה של קוד זדוני שמאפשר שליטה מרחוק במערכת ועוד.

<u>סוג האקרים במתקפת סייבר שכזו יכולים להיות:</u> "משקיעים שיש להם אינטרס במידע רגיש כדי לזכות במכרז או לדעת על קיום של נכס במיקום ובמחיר אטרקטיבי. כמו כן, אקרים ממניעים אידיאולוגיים המתנגדים למדיניות העיריה בנושאים שונים או שמעוניינים לגנוב כסף מקופת העיריה; גורמים עוינים בשעת חירום" מוסיף טרבלסי.

אריה קליינר מנכ"ל חברת NovaSens המספקת בין היתר יכולת הצפנה של מידע ואבטחה למניעת סייבר: "צמיחתם והתרחבותם של הערים החכמות מזמינות האקרים למיניהם לבצע פעולות זדוניות בעוד שרשויות המדינה כבר מוגנות בפני כך ומקצות תקציבים ומשאבים להגנה, נותרו הערים עצמן- הארגון הגדול ביותר החשוף לפגיעה וללא מתודולוגיה סדורה להגנתם. מדובר בפוטנציאל סכנה גבוה מאוד בפריצה שכזו ואין להקל ראש בכך. פריצה שכזו עלולה להוביל לשיבוש כולל של מתן שירותים לאזרח, דליפת מידע על האזרחים ופרטיהם כמו רכושם וכ"ו, הכנסת מידע שגוי על כל תושב ותושב ופגיעה במאגרי נתונים קיימים".

מה מציעות כיום החברות הטכנולוגיות?

קבוצת סופרקום פיתחה מערכת ה'SafeMobile' שמספקת שכבת הגנה לאפליקציית המובייל 'MuniCom' של הרשויות המקומיות נגד איומי סייבר (שכבת הגנה העומדת בסטנדרטים המחמירים ביותר ומשמשת בנקים, חברות ביטוח וחברות תקשורת). פלטפורמה ה'SafeMobile' מאפשרת למפתחי אפליקציות להגן בצורה החזקה ביותר מפני חדירות מובייל. בנוסף, חברת 'Safend' מספקת פתרונות הגנה רחבים לנקודות הקצה במחשבי הרשות המקומית (לרבות הצפנת המידע), כנגד איבוד מידע במכוון או שלא במכוון על ידי עובדים או אנשים חיצוניים על ידי העתקה, שליחה במייל, העלאת נתונים לענן או הדפסת מידע רגיש הכל תחת התקינות המחמירות בעולם.

חברת NovaSens לעומת זאת פיתחה יחידות קצה המיישמות טכנולוגית "קריפטוגרפיה" שמיועדת להגנה מפני התקפות סייבר מסוג כזה. יישום הטכנולוגיה יאפשר לזהות את היחידה המשדרת במהירות, לאמת את היחידה ולמנוע התחזות, שימוש במפתחות הצפנה , הגנה בעת עדכון התוכנה והגנה אקטיבית מפני ניסיונות חדירה והרס נתונים רגישים אודות התושב.

חברת סופר קום וחברת נובולוג יציגו את הטכנולוגיות שלהם במסגרת יריד MUNI-EXPO, יריד החדשנות המוניציפאלי של מרכז השלטון המקומי שמתקיים השנה לראשונה ויציג את שלל הטכנולוגיות והפלטפורמות לניהול חכם של ערים. היריד יתקיים ב24-25 לינואר בביתן 2 בגני התערוכה.

היריד יפגיש לראשונה - למעלה ממאה מציגים, שיחשפו פיתוחים וחדשנויות בפני כ – 5,000 מנהלים ומקבלי החלטות באירוע המוניציפלי הגדול והמשמעותי ביותר - המתקיים לראשונה בארץ. עוד יתקיימו במסגרת היריד, שלל כנסים מקצועיים בתחומי הניהול המוניציפאלי