מס' פרויקט	שם הפרויקט
2021-01-150	האם משתמשים במכשירים ניידים פגיעים יותר להתקפות באבטחת מידע?

מנחה אקדמי	מנחה שותף
פרופסור ליאור פינק	גב' נעמה אילני-צור

חברי הצוות		
נועה בנג'ו	ליהיא אוחיון	
benjon@post.bgu.ac.il	lihio@post.bgu.ac.il	

תקציר

בימנו מתקפות סייבר הופכות שכיחות ועולות במהדורות החדשות על בסיס יומי. הדבר נובע מכך שבעידן של ימנו זמינותו של האינטרנט והשימוש בו הולך וגובר באופן אקספוננצילי, ובמקביל מחירם של המכשירים האישיים המשמשים אותנו כמו מחשבים, טאבלטים וטלפונים חכמים, הולך ופוחת. הפרויקט יעסוק בהבדלים בשימוש בין מובייל למחשב בעת ביצוע פעולות שגרתיות שחוזרות על עצמן.

במסגרת הפרויקט ברצוננו לבדוק האם קיימים הבדלים בהתנהגות המשתמש במכשירים שונים, בתחום הפרטיות ואבטחת המידע במטרה לאפיין דפוסי התנהגות משתמש ויחסו לאיומים על מכשירו. מסקירת הספרות שביצענו השערתנו הראשונית הייתה כי השימוש בטלפונים ניידים הינו מסוכן יותר. במסגרת הפרויקט יזמנו שיתוף פעולה בין אוניברסיטת בן גוריון לחברת SAM, אשר עוסקת באבטחת מכשירים ברשתות ביתיות ובשל כך בעלת בריכת נתונים שסייע לנו במענה על שאלת המחקר.

בפרויקט מימשנו מתודולוגיה של ניתוח נתונים ובניית מודל לחיזוי הסיכוי לגלישה מסוכנת על פי משתנים שונים ובמרכזם סוג המכשיר ממנו בוצעה הגלישה. שלפנו ממאגרי החברה נתונים המתארים גלישות אשר בוצעו מ-30 רשתות שונות, ממכשירים אשר היו מחוברים לרשתות אלו במהלך תקופה של שבעה ימים. לכל גלישה ניתן דירוג מסוכנות, בטווח שבין 0 (מסוכן) ל-100 (בטוח), אשר חברת SAM מצמידה לו משירות חיצוני בשם Bright Cloud.

לצורך שליפת הנתונים עבדנו עם שני מאגרים של החברה. בריכת נתונים (שירות Athena ו-S3 של AWS) בו מאוחסנים נתוני הגלישות לפי מכשיר ורשת, ובסיס הנתונים של החברה אשר בו מאוחסנים דירוגי האתרים. לאחר מיזוג השליפות ביצענו ניקוי של הנתונים. במסגרת הניקוי ביצענו אנונימיזציה של מזהים אישיים, הסרת כתובות האתרים ושמירת דירוג המסוכנות בלבד. הוחלט להמיר את דירוג האתרים לבינארי, גלישה בטוחה או מסוכנת (דירוג סף-40) מכיוון של ששירות Bright Cloud מסווג גלישה מסוכנת כגלישה מתחת ל-40 ושחברת SAM חוסמת אתרים בעלי דירוג מתחת לסף זה.

לאחר הכנת הנתונים ביצענו ניתוח תיאורי במספר ממדים: זמן, רשת, מצב המכשיר ברשת (קבוע או מזדמן), מערכת הפעלה וסוג המכשיר. בשלב זה עלה נתון מעניין אשר עמד בניגוד להשערתנו הראשונית והוא כי למרות שגלישות ממחשבים היוו כ-20% מכלל הגלישות בסט הנתונים, מתוך הגלישות המסוכנות בסט הנתונים, כ-70% בוצעו ממחשבים.

בשלב הבא ביצענו בדיקות למציאת מובהקות של הקשרים בין המשתנים ודירוג הגלישה. מבדיקת שילובים בין המשתנים ובדיקת סוגי מודלים שונים במטרה ליצור מודל לחיזוי מסוכנות גלישה, בחרנו במודל רגרסיה לוגיסטית מעורבת אשר מכיל את המשתנים סוג המכשיר, מספר מכשירים ברשת, אחוז הטלפונים ברשת מכלל המכשירים ומצב המכשיר ברשת.

מהניתוחים שבוצעו ומתוצאות המודל הנבחר עולה כי גלישות המבוצעות ממחשבים הינן בעלות סיכון של פי 4.02 להיות גלישות מסוכנת לעומת גלישות המבוצעות מטלפונים ניידים ולכן שימוש במכשיר זה עלול לחשוף את המשתמש באופן ניכר יותר למתקפות סייבר. בנוסף, מצאנו כי לגלישות ברשתות בהן מספר המכשירים גבוה יותר גם כן מעלות את הסיכוי של הגלישה להיות מסוכנת. מתוך מסקנות אלו אנו ממליצות לחברת SAM להגדיר רמת סיכון שונה עבור מכשירי מובייל ומחשבים.

מילות מפתח: מערכות מידע, ניתוח נתונים, סייבר, התנהגות משתמש, מחשב, מכשירי מובייל