בקרוב

DailyMaily גיליון 4839 יום ב', 9.3.2009
מו"ל ועורך אחראי: **פלי הנמר** | עורך ראשי: **יהודה קונפורטס** | עורך: **אור יעקב** | סגן עורך: **-**

פורום SD

"יש לחשוב על אבטחת מידע בכל הליך הפיתוח"

"במעבר מאבטחת תשתית לאבטחת יישומים, המפתחים מגלים שיש מגוון רב של דרכים שבהן ניתן לפגוע ביישום", הוסיף אופיר זילביגר, מנכ"ל SECOZ, במפגש פורום מנהלי הפיתוח של קהילת אנשים ומחשבים - SD, שנערך ביום ה' ● לדבריו, "חשוב להיות מודעים לאותן דרכים, כדי ליצור סביבה מוגנת יותר מכפי שהיא כיום"

רן מירון, מערכת DailyMaily, ThePeople

"אבטחת המידע לא הייתה קשורה לפיתוח במשך זמן רב מידי, עובדה שיצרה בעיות אבטחה קשות בעולם האינטרנט וביכולת של הארגונים להגן על עצמם מפני התקפות מבפנים", אמר **אופיר זילביגר**, מנכ"ל חברת הייעוץ **SECOZ**, במפגש SD - פורום מנהלי הפיתוח של קהילת **אנשים ומחשבים**, שנערך במלון קראון פלאזה בתל אביב.

"במעבר מאבטחת תשתית לאבטחת יישומים", הוסיף, "המפתחים מגלים שיש מגוון רב של דרכים שבהן ניתן לפגוע ביישום. חשוב להיות מודעים לאותן דרכים, כדי ליצור סביבה מוגנת יותר מכפי שהיא כיום". זילביגר אף סקר בפני חברי הפורום את התפתחות עולם האינטרנט, האיומים שצמחו והמעבר מאבטחה ממוקדת תשתיות לאבטחה ממוקדת יישומים. "האקרים רבים עושים שימוש בנקודת החולשה שב-User input כדי להבין את היישום", אמר, "לפגוע בו ולעשות עליו מניפולציות. המפתחים מתמקדים בטעויות השכיחות שעושים אנשים תמימים בממשך היישום. זה טוב ויפה, רק שנדרש גם להיות ערים לפעולות לא תמימות, כמו הזנת ערך שלילי בהעברה מחשבון לחשבון בעולם הבנקאי".

לדבריו, "ההאקרים אף פיתחו טכניקות מתקדמות לצורך תשאול היישום לשימושים נוספים, שהמפתח ודאי לא התכוון לאפשר את קיומם. הדוגמה המוכרת ביותר היא שימוש בשורת ה-URL ושינוי פרמטרים שמופעים לאחר תו סימן השאלה". הוא הוסיף, כי "דרך נוספת לחדור ליישום קשורה בנושא ניהול טעויות המשתמש. אנשי הפיתוח דואגים בדרך כלל לכך שהיישום יחזיר למשתמש כמה שיותר מידע הנוגע לטעות שביצע. הבעיה היא שפעמים רבות מידע זה מגיע למשתמש עם פירוט לגבי הסביבה שבה מתנהל היישום ופירוט נוסף, שאותו מנצל ההאקר לצורך כוונותיו הזדוניות". זילביגר סיכם את הרצאתו בנימה אופטימית, תוך שציין מספר כלים המאפשרים לבצע תהליכים מיטביים בעולם בדיקות הקוד לצורך הידוק אבטחת המידע ביישומים.

אלדד גלקר, מנכ"ל קבוצת **צ'יף**, המתמחה בהצלת נתונים, הציג בחלק הראשון של הרצאתו נתונים הקשורים לתחום התמחותו - פגיעויות וכשלים של דיסקים. לדבריו, רוב המידע בעולם מצוי בדיסקים, והמחיר הממוצע לג'יגה-בייט בדיסק ממשיך לרדת בהתמדה. זה עומד כיום על 47 אגורות לג'יגה-בייט. עוד סיפר גלקר למשתתפים על מקרים קיצוניים של נזקים לדיסקים כתוצאה משיטפונות, שריפות, קריסת מבנים ורעידות.

עם זאת, הוא ציין, כי 55% מהבעיות בדיסקים קשורות דווקא באיכות ירודה של חומרה. "**גוגל** עשו לאחרונה מחקר לבדיקת כשלים בדיסקים, אולי המחקר האובייקטיבי הראשון שנעשה אי פעם. הממצאים היו קשים: בתקופה של חמש שנים הושבתו בגוגל 100 אלף דיסקים. 3% שרדו רק שלושה חודשים, ללא קשר ליצרן מסוים או לטכנולוגיה. 80% מהדיסקים שרדו שלוש שנים, ורק 20% שרדו שנתיים נוספות".

בחלק השני של ההרצאה הציג מנכ"ל צ'יף את ה- Personal Down Time - פתרון שפיתחה החברה לצמצום הזמן הנדרש לשם שחזור קוד ומידע נוסף שניזוק, נמחק או נעלם. לדבריו, פתרון זה פותח כמענה לקושי בהפקת ערך אמיתי מהגיבויים המבוצעים בארגון.

טל פרנז'י, מהנדס תוכנה בגוגל ישראל, הציג את App Engine, שירות חדש יחסית שמציעה החברה, המיועד למפתחי אפליקציות הרוצים להשתמש בתשתית שמעמידה לרשותם גוגל כדי להריץ יישומים המפותחים, בשלב זה, אך ורק בשפת פייטון. ה-SDK (ר"ת Software Development Kit) זמין בכל מערכות ההפעלה המובילות.

עד כה אפשרה גוגל לקבל נפח אחסון של כמה מאות מגה-בייט בחינם, וכן כוח מיחשוב המאפשר צפייה בכחמישה מיליון דפי רשת מדי חודש. "עם App Engine, גוגל מציעה ערכת פיתוח שלמה שעושה שימוש בטכנולוגיות מוכרות לצורך בנייה ואירוח של אפליקציות וב", אמר פרנז'י. "המפתח יכול להתחיל לעשות שימוש בחינם, ובמידה שיידרשו לו עוד כוח מיחשוב ושירותים נוספים - אלה יהיו זמינים עבורו במחירי שוק תחרותיים". עם זאת, הוא ציין, כי היישומים המפותחים במסגרת השירות יהיו אמנם מוגנים על ידי התשתית המאובטחת של גוגל, אך רמת אבטחת היישום עצמו תישאר בידי מפתחי היישום.

יניב ינקוביץ, מנהל פרויקט בחברת **אורבוגרף**, חברת תוכנה בבעלותה של **אורבוטק**, הציג בעיות בעולם אבטחת המידע הבנקאי והמענה שפיתחה אורבוגרף לבנקים מובילים בעולם, כמו סיטיבנק. בין הפתרונות שהוצגו היה ולידציה להמחאות וזיהוי הונאות בתחום ההמחאות, באמצעות מוקד מרוחק המופעל מהודו.

בניית אתרים Daronet