שלום TELAVIV
SHALOMTELAVIV.COM

ירון בלכמן, PwC ישראל: "היקף המתקפות על מערכות SCADA הוא פי 100 ממה שמתפרסם"

"המערכות האלה מצויות בכל מקום: מערכות מים, תחנות חשמל, רשתות גז, רמזורים, רכבות, קווי יצור, מתקני שעשועים, מכשירים רפואיים ועוד, ובכולן יש פרצות אבטחה", אמר בלכמן, מנהל תחום סייבר ואבטחת מידע בקבוצת הייעוץ של החברה • שי קידר, מנכ"ל Vsecure: "הסבירות לתקיפת מערכות SCADA קיימת בכל רגע נתון"

מאת יוסי הטוני, 24 בדצמבר 2013, 11:34

פורום CISO

"היקף המתקפות על מערכות SCADA הוא פי 100 ממה שמתפרסם - כך מעלים המומחים. המערכות האלה מצויות בכל מקום: מערכות מים, תחנות חשמל, רשתות גז, מערכות רמזורים, רכבות, קווי יצור, מתקני שעשועים, מכשירים רפואיים ועוד, ובכולן יש פרצות אבטחה", כך אמר **ירון בלכמן**, מנהל תחום סייבר ואבטחת מידע בקבוצת הייעוץ של **PwC** ישראל.

בלכמן דיבר במסגרת פורום CISO, מועדון אבטחת המידע של **אנשים ומחשבים**. המפגש נערך אתמול (ב') במלון שרתון בתל אביב והנחה אותו **אבי וייסמן**, מנכ"ל **שיא סקיוריטי**.

לדברי בלכמן, "ככלל, מערכות ה-IT מאובטחות, אלא שהבעיה והאתגר הם באבטחת מערכות SCADA". הוא ציין כי "השינויים הטכנולוגיים ב-15 שנים האחרונות משמשים את התוקפים והופכים אותם מהירים יותר. על מנהלי אבטחת המידע הארגוניים להיות מודעים לאיום - ממדינות תוקפות, מפשע קיברנטי מאורגן ומיריבים עסקיים".

"כיום, חדר הבקרה של מפעל יצרני מלא מסכי מחשב ומהווה חלק מתשתית ה-SCADA שמטרתה לנהל את המערכות לבקרה, לקבלת מידע ולשליטה עליהן. ראשי התיבות הן Supervisory Control And Data Acquisition - מערכות המשמשות לפיקוח, שליטה ואיסוף נתונים. המערכות מורכבות מ-RTU ו-PLC, רכיבים לוגיים לשליטה, המודדים נתונים וממירים אותם למימד דיגיטלי. RTU קורא את הנתונים מרחוק", אמר.

בלכמן עמד על ההבדלים בין SCADA ו-IT: "מערכות IT בעלות זמינות של 99.5% הן סבירות ומערכות SCADA דורשות 100%, אין להן הגנה, הטלאות, עדכוני אבטחת מידע ובדרך כלל אין עליהן אנטי וירוס. הציוד המדובר מתיישן, כמות הנוזקות כלפיהן גדלה וכמות המתקפות נגדן ונגד היצרניות - אף היא גדלה".

"אנחנו צורכים SCADA מרגע ההשכמה"

שי קידר, מנכ"ל **Vsecure**, אמר כי "אנחנו צרכנים של מערכות SCADA מרגע שאנחנו קמים בבוקר ושמים מים בקפה דרך הרמזורים שיש בדרכנו לעבודה ועד להפעלת מערכות מיזוג האוויר במשרד. מערכות הכריזה וכיבוי האש - גם הן SCADA".

לדבריו, "הסבירות לתקיפת מערכות SCADA היא כמו הסבירות למתקפות סייבר - בכל רגע נתון. עלינו לשאול האם אנחנו מוכנים לקראתן? האם יש מערכות איתור וגילוי? והאם יש יכולת תגובה?". הוא הוסיף כי "מה שחשוב בעולם ה-IT הוא ההגנה על המידע ובעולם ה-SCADA הוא הזמינות".

בהמשך ציין קידר כי הפגיעויות העיקריות במערכות בקרה תעשייתיות (ICS) הן "בפרוטוקולי תקשורת, בארכיטקטורה, בניהול הטלאים, באותנטיקציה, באי ההיערכות של הספקים, בגרסאות ישנות, בפיתוח יישומים בצורה מיושנת ובריבוי פרוטוקולים".

"לכן", אמר, "נדרשים תכנון אסטרטגי להגנה עליהן, בחינת איומים רלוונטיים לפי כל מגזר, בדיקת היתכנות האיום ותכנון פתרונות לרשתות SCADA עם אפיון נקודתי". הוא ציין כי פגיעה במערכות SCADA המביאה להשבתה עולה מאות אלפי דולרים לשעה ומעלה בעיות בעמידה מול הרגולטור.

"הלוחמה הווירטואלית מתאפיינת בחתימה נמוכה"

אופיר חסון, מייסד ומנכ"ל **CyberGym**, סיפר כי הקים את החברה לאחר שנות עבודה בראמ"ם שבשב"כ. הוא אמר כי בניגוד ללוחמה הפיזית, זו הווירטואלית מתאפיינת בחתימה נמוכה. "עולם הסייבר, בשונה מלחימה צבאית רגילה, הוא בעל מאפיינים אחרים: ההיערכות לפיגוע קיברנטי לא דורשת משאבים וזמן רב, אין חשש לפגיעה. המרוץ הטכנולוגי מתיש ומסייע ל-'רעים'. מרחב הסייבר הוא בלתי נודע, בלתי נראה, לא צפוי, לא מתוחם וגם לא נגיש", הוסיף.

חסון אמר כי "תולעת, בניגוד לטיל, לא ניתנת למיפוי. גם אם ידוע שהיא נמצאת במערכות, ייתכן שלא ניתן יהיה לדעת מי שלח אותה. המשלוח שלה פשוט וקל, ניתן לנתח אותה ו-'להשיב' אותה לשולח".

הוא סיים בהציגו את זירת האימונים להתמודדות עם איומי סייבר שהקימה CyberGym עם **חברת החשמל** שלדבריו מספקת "הדמיה מלאה של התהליכים התפעוליים, עם התנהלות אמיתית בסביבה מבוקרת ומפוקחת וחוויה של מנעד התקפות רחב".

"ההבדלים בין מערכות IT ו-SCADA - מהותיים"

רותם בר, מהנדס תקשורת ואבטחת מידע למערכות קריטיות ב**לימפוקס**, אמר כי "ההבדלים בין מערכות IT ו-SCADA מהותיים. הם נעים החל מרמת ההתייחסות להגדרות אבטחה, כמו תפוגה של סיסמאות, עבור בדרישה בסיסיות מציוד ותכנון של רשת הארגון ומערכות האבטחה וכלה בדרישות התפעול השוטף של מערכות אלה, כגון הדרישה להתחברות מרחוק".

אהרון יוסף, מנהל פיתוח עסקי ב**סורספייר** (SourceFire) ישראל, דיבר על פתרונות הגנה פרקטיים ברשתות SCADA. הוא תיאר כיצד יש לבנות מתודולוגיות של הגנה על רשתות בשישה שלבים: "פיתוח מתודולוגיה של הגנה, תוך דגש על נראות; פיתוח נראות בזמן אמת, על ידי הטמעת יכולות סריקה של ציוד SCADA; ניטור תעבורה; בדיקת המשתמשים במערכות; ניטור תעבורה חיצונית מחוץ לרשת; ואיתור פעיל של ניסיונות פריצה ברמת רשת ותחנות קצה".