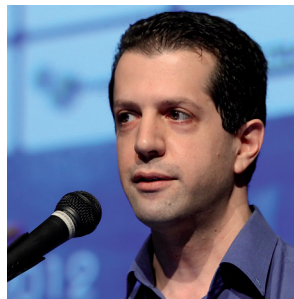


תשתיות קריטיות בקלות ולגרום לנזקים גדולים. המדובר באתגר חשוב בפניו ניצבים הקברניטים", כך אמר **שי צלליכין**, CTO קבוצת קומסק. צלליכין הציג מגמות בעולם מערכות משובצות מחשב והתקפות מבוססות חומרה. לדבריו, "ראינו כמה התקפות ואירועים בעולם מערכות בקרה תעשייתיות, SCADA, בתקופה האחרונה. כך, בחודש נובמבר האחרון חשבו שרוסיה תקפה מתקנים ומערכות מים בארה"ב. חקירה העלתה כי המדובר במתקפת שווא, אף שמקור התקיפה היה כתובת IP רוסית. הסתבר כי אחד מהעובדים - כשהיה בחופשה ברוסיה, התחבר למערכת מרחוק. המערכת קרסה והאירוע יצר 'הייפ' תקשורתי". לדבריו, "האירוע המחיש כמה קל לתקוף תשתיות קריטיות מרחוק".

צלליכין הציג עוד דוגמאות אחרות של פרויקטים שחקרו מערכות ובקרים של תשתיות קריטיות לאומיות, והמסקנה העולה מכלל המחקרים והדו"חות היא "שיש בהן כמות חולשות מאד גדולה". כך, אמר, "במחקר שנעשה על בקרים, ביניהם של סימנס, נתגלו 'דלתות אחוריות', יכולות חדירה, יכולות תכנות מחדש של בקרים, בדיוק כפי שקרה במקרה של סטוקסנט". "מערכות שו"ב ומערכות משובצות מחשב, אשר פועלות במתקני תשתיות קריטיות, הן מערכות ישנות במקרים לא מעטים", אמר צלליכין, "הדבר גורם לכך שבהכרח רמת אבטחת המידע שלהן היא לא אחידה. לכן רמת החוסן שלהן מפני מתקפות קיברנטיים מתוחכמות היא נמוכה".



אלכס נשטיין



שי צלליכין

שכבת הגנה דלה

צלליכין הציג כמה דוגמאות של מערכות SCADA אמריקניות, שהיו מחוברות לרשת ומוגנות ברמת אבטחה מאד נמוכה. בין השאר הוא הציג מערכת של תשתית קריטית, שכל שכבת ההגנה עליה הסתכמה בשלוש אותיות ברירת מחדל בסיסמה.

אתגר נוסף, אמר, "הוא לטווח הארוך. אנו צופים כי תהייה התקפות ברמה נמוכה יותר, והיא ברמת השבבים, לצד פעולות תקיפה קיברנטית בסביבת מערכות וירטואליות. כך, אם נשתל סוס טרויאני בטלפונים החכמים של עובדי הארגון, גם יכולת האיתור היא אפסית וגם יש לתוקפים יכולת להשבית את כל הטלפונים בשליטה מרחוק, או להשבית את כרטיסי הרשת או מחשבי הארגון".

לפיכך, אמר צלליכין, "נדרש לשנות את התפיסה לגבי האופן בו יש לאבטח את המערכות. יש להקפיד על ניתוק מעולם האינטרנט. יש להיות מודע למגוון הסיכונים ולבצע בחינה של הסיכונים הללו ולהכיר את החולשות שבמערכות. המערכות של תשתיות קריטיות הן 'שבירות' ורגישות, וארגונים אינם ממהרים לגעת בהם. למרות זאת נדרש להגן עליהן ולעדכן את ההגנה עליהן".

"ראינו לא מעט מקרים, בארה"ב ובארצות שונות בעולם", סיכם, "של תשתיות קריטיות שהתגלו בהן פרוצות או שלחילופין הן היו מחוברות לרשת בצורה לא מאובטחת. אם לא ייעשה צעד מיידי לניתוק מערכות אלה מהאינטרנט ולהעלאת רמת החסינות מפני מתקפות סייבר - אנו עלולים לראות נזקים ברמה הרבה יותר גבוהה".

"מתקפות מזיקות בהרבה, שהציבור טרם נחשף אליהן"

"כמות המתקפות גדלה באופן אקספוננציאלי, לצד הגידול ברמת התחכום שלהן. מה שפחות ידוע ויותר חשוב הוא העובדה, כי כמות

"עולם הסייבר החל בשנות ה-80", ציין. "הווירוסים הראשונים הופיעו במקביל לכך שהתאגידים, בעיקר אלה הפיננסיים, הבינו שביכולתם להגדיל את הכנסותיהם על ידי הקמת אתר אינטרנט, ובכך האתרים הפכו להיות מוקד לאיומים. בתחילת שנות ה-2000, עיקר ההשקעות של קרנות ותאגידים בעולם האבטחה היה תוצאה של פעילות האקרים ושיתוף הפעולה שלהם עם ארגוני פשע. כך גם עד היום. על מנת להוזיל עלויות, מדינות עברו מהתבססות על טכנולוגיות ייחודיות להתבססות על טכנולוגיות מיינסטרים. או אז, בעיות האבטחה חדלו להיות בעיות של התאגידים והפכו להיות בעיית המדינה".

הוא הוסיף, כי "עולם הסייבר הוא עולם שטוח. הרבה ממדים בו אינם רלוונטיים, בהם המימד הפיזי ומימד המרחק. ההתנהגות של גוגל ב-2010, בעקבות הפריצה לשרתיה בסין, מעידה שהכסף מדבר. האינטרנט נתפס כנשק פוליטי. סין היא המעצמה מספר 1 בעולם בתחום הסייבר ויש לה 150 האקרים שמונה בין 100 ל-150 אלף איש. למרות זאת, יש קושי לחבר ולעשות את הזיהוי של התוקפים עם מדינות".

כרמלי ציין כמה סוגי מתקפות שמבוצעות, ביניהן מניעת שירות (DoS) על ידי יצירת עומס, השחתת אתרים והשתלטות על מערכי ניתוב, מה שגורם לשיתוק התעבורה ברשת. הוא אמר שיש

"אינסוף מתקפות סייבר" וציין כמה מהמפורסמות שבהן, כולל זו שקרתה באסטוניה, שהיא מדינה מבוססת מיחשוב, ב-2007. לאחר שהוחלט להזיז את פסל החייל האלמוני ממרכז הבירה, טאלין, למקום צדדי, חוותה אסטוניה מתקפות קיברנטיות בלתי פוסקות מצד רוסיה - מה שהביא לשיתוק החיים בה במשך שבועות. "האם לנו זה יכול לקרות?", שאל כרמלי ומיד השיב: "יכול".

"סייבר זה לא במ"מ"

כרמלי עמד על האבחנה בין סייבר וביטחון מערכות מידע (במ"מ). "סייבר זה לא במ"מ", אמר. "דמיינו תקלה במערכת טלפוניה ארצית שהיא תוצאה של תקיפה שמביאה להשבתה. במקביל, דמיינו אירוע רב נפגעים, כגון הצתה. התקלה הגדולה בסלקום התרחשה יום אחד לפני השריפה בכרמל. חישוב איך היו כוחות הביטחון מטפלים בשריפה כאשר שלישי מהטלפונים מושבתים".

לדבריו, "עולם הסייבר הוא אמיתי, הוא לא המצאה של אנשי שיווק ומכירות של ספקיות אבטחת מידע. הוא חיבור של עולם הבמ"מ להיבט של יצירת איום על תאגידים, על גופי תשתיות לאומיות קריטיות ועל מדינה". "סייבר זה לא מימד, זו פלטפורמת לחימה", הוסיף. "הוא יכול לעמוד בפני עצמו או כחלק ממכלול רחב יותר של מתקפות שלא במימד הסייבר". הוא תיאר את מעגלי ההגנה השונים שנדרש לבנות על מערכות המיחשוב, וציין כי במעגל הניטור מתחיל החיבור לסייבר, ובנוסף נדרש איתור אקטיבי.

"לתוקפים מספיק סדק אחד על מנת לתקוף, ואילו למוותקפים נדרשת הרמטיות מוחלטת", סיכם כרמלי. "על מנת להדביק את הפערים הללו יש לפעול לא רק בהיבט הטכנולוגי אלא גם בתחומי ההדרכה, החינוך ושינוי התרבות. ישראל עושה לא מעט על מנת לבצע זאת".

"ניתן לתקוף תשתיות קריטיות בקלות"

"מערכות הגנה ושו"ב של תשתיות קריטיות לאומיות הן לעיתים מיושנות ולעיתים אף מחוברות לרשת האינטרנט. בשל כך ניתן לתקוף