איך לעבור מאבטחת מידע מסורתית להגנה מפני APT?

"מערכות השו"ב מבוססות טכנולוגיה ישנה, ויש ריחוק בין מנהל הייצור והצורך באבטחת מערכות אלו", אמר יגאל גואטה, משנה למנכ"ל Prevision ◆ לדברי שי קידר, יועץ אבטחה לתשתיות קריטיות ו-SCADA, "במערכות ה-SCADA יש חשיבות רבה יותר לביצועים ולמהירות מאשר לסודיות המידע. יש מעט בקרות יחסית ל-IT"

יוסי הטוני

"הכי כדאי היה לקחת את מערכות השליטה ובקרה של תשתיות קריטיות ולטמון אותן עמוק באדמה באופן מבודד. אלא שנדרש להגן עליהן בצורה הגיונית על מנת שהמערכות תוכלנה לתפקד", אמר **יגאל גואטה**, משנה למנכ"ל Prevision, בפורום CISO מקבוצת אנשים ומחשבים, שהתכנס במלון שרתון שבתל אביב. את המפגש הנחה אבי וייסמן, מנכ"ל See Security.

ההגדרה המקובלת לסייבר, אמר גואטה, היא "מרחב אלקטרוני של רשתות מחשבים בהן יש תקשורת מקוונת". לעומת זאת, הגדרתו היא "כל מדיה המכילה אותות אלקטרוניים". לדבריו, יש דימיון בין עולם אבטחת המידע של העבר ובין עולם אבטחת הסייבר כיום, לצד שלוש יכולות חדשות, בהן רמת מודעות גבוהה של התוקף ושל המגן לאחריו. רמת המודעות, אמר, באה לידי ביטוי במספר תחומים, בהם בנק המטרות, משמע כל ציוד מבוקר מחשב, ובאמצעים - מודיעין איכותי, כלים ייעודיים, צוותים ייעודיים, לשילוב של אמצעים ממוחשבים, פיזיים ואנושיים.

לצד המודעות, ציין, יש יכולות גבוהות יותר, עקב כניסת גורמים בעלי משאבים כמעט בלתי מוגבלים. "נכנסו לתחום הסייבר מומחים משולבים מתחומים שונים. יש שימוש בתשתיות ציבוריות ותשתיות ענק, ויש הכשרות מקצועיות. ההיבט השלישי, ציין, הוא רמת המוטיבציה הגבוהה מאד: "המדינה שרויה במעין מלחמה, אין לה ברירה והיא חייבת להתמודד מול אויב הנחוש לחסלה".

מערכות שו"ב, אמר גואטה, "הן מערכות מבוססות מחשב, ומחשבים תעשייתיים מבוססי לוגיקה - מפלס המים עלה, המשאבה עובדת וכו'. מערכות אלה כמעט ואינן מכילות אמצעי אבטחת מידע".

התוקפים, אמר, "מחפשים יעד אטרקטיבי, גדול, שתקיפתו תעורר רעש גדול ונזק רב. המערכות מבוססות טכנולוגיה ישנה, פרוטוקולים קנייניים, ויש ריחוק בין מנהל הייצור והצורך באבטחת מערכות אלו. על מנת לפגוע בהן נדרש בנוסף לרקע של ההאקר גם ידע הנדסי. כדי שהמתקפה תצלח, נדרש לקבל מידע פנימי. קוד התקיפה חייב להכיל יסודות של שליטה".

הוא אמר, כי על התוקפים להחליט מה רצונם להשיג: הורדת רמת שירות, שיבוש, שינמוך, חדירה לצורך פעילות עתידית, הרס או בדיקת כלים. החלטה נוספת, ציין, היא מהו סוג המתקפה: מניעת שירות - בכל הרמות, מערכות השו"ב, מערכות ההפעלה, היישומים, או נזק למידע ולנתונים, נזק פיזי, או בניית בסיס לשימוש עתידי.

"אם אינך רואה דבר באנטי וירוס ובפיירוול - זה לא אומר שאינך מותקף", סיכם גואטה. "אם יש בעיה מתמשכת נטולת פתרון תפעולי, חפשו את הבעיה במקום אחר".

SCADA

שי קידר, יועץ אבטחה לתשתיות קריטיות ו-SCADA, פתח בהסבר מהו מערכות אלה: "מערכות תעשייתיות לניהול פעולות ותהליכים בזמן אמת, בקרות פיקוח ואיסוף מידע, ניהול מנופים, מגופים, ממסרים משאבות וכו'". המערכות, אמר קידר, מצויות בכלל המגזרים - כימיקלים, אנרגיה, גז, מים ועוד. "תשתיות מיחשוב קריטיות חיוניות הן מבוססות SCADA", אמר, "השבתת מערכות אלה עלולה לגרום נזק ברמה הלאומית ועלולה לפגוע בחיי אדם".

בעבר, אמר קידר, "מערכות ה-SCADA היו חומרה ותוכנה ייעודית ליצרנים. היה מספר רב של יצרנים ורכיבים, המערכות היו סגורות, ללא אימות ועם פרוטוקולים ישנים. כיום, המערכות הן בעלות כלי תקשורת מתקדמים, הן משולבות עם רשתות ה-IT, יש חיבורים וקישוריות Wi-Fi ואינטרנט, ויש פרוטוקולים Over TCP".

רשתות ה-SCADA, אמר קידר, "פגיעות יותר מרשתות IT: מאחורי כל רשת יש מפעיל, מודעות העובדים לוקה בחסר, יש קושי ביישום מדיניות אבטחה, יש תחלופה גדולה של עובדי בקרה, בחלק מהמערכות אין סיסמאות, אי אפשר לעדכן את המערכות. הן בעלות מחזור חיים ארוך של 15-20 שנים, ויש חשיפה למגוון פגיעויות במערכות מבוססות חלונות. הפרוטוקולים פשוטים ובעלי מעט הגנה, אין הצפנה ברשת, והן חשופות למגוון סוגי התקפות. הרשתות נדרשות להיות מבודדות אך בפועל הן מחוברות". לסיכום אמר, כי "במערכות ה-SCADA יש חשיבות רבה יותר לביצועים ולמהירות מאשר לסודיות המידע. יש מעט בקרות יחסית ל-IT".

חתם את המפגש **משה ישי**, מנכ"ל קומסק ייעוץ מקבוצת קומסק.