TOPCO
It's all about control

בעידן ההאקרים, עד כמה מאובטח בקר ה-PLC שלכם?

הבה נודה בכך - אנחנו חיים בעידן ההאקרים, ובמשחק החתול והעכבר בזירת לוחמת הסייבר, ההאקרים צברו לזכותם כמה נקודות מרשימות. החל ממתקפת WannaCry שחשפה את אתר אשלי מדיסון ועד ל"גניבת בחירות" לכאורה, האקרים מנצלים לרעה חולשות ובונים לעצמם שם רע במיוחד.

מחקר שנערך לאחרונה על ידי מרכז המידע לגניבת זהויות, מצא כי בשנת 2016 חברות וסוכנויות ממשלתיות אמריקניות חוו 1,093 פריצות למערכות שלהן. זהו שיא חדש וגידול של 40% בהשוואה ל-780 הפריצות שנרשמו ב-2015. אבל לא מספר ההתקפות הוא שמדהים, אלא היקפן והנזק כתוצאה מהן.

במתקפה של 2014 על הום דיפו, הצליחו האקרים לפרוץ לעמדות הקופות בשירות עצמי של החנות ולגנוב פרטי דוא"ל וכרטיסי האשראי של מעל 50 מיליון לקוחות. חמישים מיליון! ההערכה היא כי מתקפה בודדת זו תעלה להום דיפו לפחות 179 מיליון דולרים בפיצויים, וחלק מההערכות המשקללות עלויות משפטיות ותשלומים חסויים גבוהות אף יותר.

הפריצה להום דיפו הייתה רק אחת מקריאות ההשכמה הרבות עבור העולם התאגידי, אך למרבה הצער גם חלק מהסוכנויות הממשלתיות הגדולות ישנו. מוערך כי הפריצה לנתוני ה-IRS ב-2015, במהלכה חדרו האקרים למערכת "Get Transcript" של רשות המסים האמריקנית והשיגו גישה ליותר מ-700,000 חשבונות שהכילו מידע פיננסי רגיש ומספרי ביטוח לאומי, עלתה למשלם המסים 50 מיליון דולר בשל תביעות מזויפות.

אין דרך אחרת לומר זאת - פצחנות (hacking) הפכה להיות עסק רווחי מאוד. זו הסיבה שבגללה האקרים כל כך מתמידים בה ומשפרים ללא הרף את השיטות שלהם. השיטות נעות משליחת דוא"ל "פישינג" פשוט, אשר מפתה את הקורבנות למסור מידע אישי להודעת דוא"ל מזויפת (על פי מרכז המידע לגניבת זהות, הונאות מסוג "פישינג" היוו כ-56% מכלל המתקפות בשנה שעברה), דרך מתקפות מניעת שירות (DOS), אשר מנסות ליצור עומס-יתר בתעבורה לאתר כדי לגרום לו לקרוס, וכלה בגניבת קובצי cookie. רוב הסיכויים שאתם מכירים את הונאות הפישינג, כי דומה שלכולנו יש קרובים רחוקים בניגריה שהשאירו לנו ירושה, או שגם לכם, כמוני, יש חשבון PayPal עם בעיה ש"אוטוטו" תגרום להקפאה שלו.

האקרים תרים ללא הרף אחר דרכים וטכניקות חדשות שאינכם מכירים עדיין. כמה מהטכניקות האלה אף יכולות להגיע ממקומות בלתי צפויים, כפי שניתן לראות במתקפת הכופר WannaCry ששוגרה לאחרונה.

מתקפת WannaCry

מתקפה זו התאפשרה בזכות פריצה לנתוני הסוכנות לביטחון לאומי (NSA). סוכנות ה-NSA גילתה לאחרונה חולשה במערכת ההפעלה Windows®, שמחדירה "חלון" (תרתי משמע) בלתי מזוהה

למערכות מחשב ברחבי העולם. במקום לדווח על הפגיעות, הסוכנות תייקה אותה כאמצעי לאיסוף מודיעיני בעתיד. לרוע המזל, קבוצה של האקרים שמכונה Shadow Brokers גנבה כמות של מסמכי NSA והפיצה אותם באינטרנט. מסמכים אלה הכילו פרטים על החולשות של Windows והובילו ליצירת הנוזקה WannaCry, שההערכה היא שמקורה בקוריאה הצפונית. עד כה WannaCry פגעה ביותר מ-200,000 מחשבים ב-150 מדינות ברחבי העולם, כשהיא נועלת את הגישה של אנשים וחברות לנתונים שלהם ודורשת כופר כדי להחזיר את הגישה.

מה לגבי בקרי PLC ?

האקרים, ובמיוחד כאלה הממומנים על ידי מדינה, הם אקטיביים מאוד והופכים בהדרגה נועזים יותר. הם ממומנים היטב ומסוגלים להוציא לפועל מתקפות ברמת תחכום עולה. האקרים בחסות מדינות אינם מתמקדים רק ברווחים כמו האקרים של עולם הפשע המאורגן. המטרות שלהם כוללות גם תשתיות או כלכלה של מדינה יריבה.

עבור המדינות הסוררות, רשת החשמל, מתקני טיפול במים, מערכות צבאיות או אתרים גרעיניים הם חלק מבנק המטרות האפשריות. למרבה הצער, אחת הטכניקות שאפשר לנצל כדי להקל על ביצוע מתקפות כאלה כבר זכתה לפרסום רב, וכן, היו מעורבים בה בקרי PLC.

וירוס סטקסנט (Stuxnet), שנחשב למיזם אמריקני-ישראלי משותף, שימש כדי לתקוף את בקרי ה-PLC של חברת סימנס במתקן הגרעין האיראני בנתנז. הסברה היא שהווירוס חדר למתקן הגרעיני דרך כונן USB. ברגע שהוחדר, סטקסנט פגע בבקרי ה-PLC של המתקן, כשהוא אוסף מידע וגורם לצנטריפוגות המסתובבות לצאת מכלל שליטה ולהשמיד את עצמן. לפי הדיווחים, סטקסנט הרס כמעט 20% מצנטריפוגות הגרעין של איראן. למרות שלכאורה מתקפת סטקסנט נועדה לפגוע ביכולות הגרעיניות של ממשל סורר, היא סיפקה דרכי פעולה חדשות גם למי שירצה לבצע בעצמו הרס כזה.

מחקר על וירוס סטקסנט שנערך על ידי קבוצת המחקר של SAP בגרמניה, הגיע למסקנה כי הווירוס היטיב להוכיח כיצד מתקפת סייבר ממוקדת מאוד ומתוחכמת במיוחד היא דבר אפשרי. המחקר גם מצא כי התכנון והארכיטקטורה של סטקסנט אינם ייחודיים לדומיין, וכי בעזרת כמה שינויים והתאמות ניתן להפכו לפלטפורמה לתקיפת מערכות אוטומטיות אחרות, כמו למשל בתחום כלי הרכב או של תחנות כוח.

בקרי PLC מאובטחים

במשך שנים רבות שמר מגזר התעשייה על ניתוק מהעולם החיצוני, כשהוא מוותר על תקשורת פתוחה לטובת אמצעים קנייניים פנימיים. סוג כזה של תקשורת סיפק רמה של ביטחון מובנה מפני עיניים סקרניות או כוונות זדון.

אך לאור ההתקבלות והגאות שחווה ה-Ethernet לאחרונה בעולם התעשייתי, ולנוכח הרצון העכשווי לחבר כמה שיותר "דברים" באמצעות ה-Ethernet ו"האינטרנט התעשייתי של הדברים" (IIoT), התעשייה פגיעה כיום יותר מתמיד.

בעולם המחובר של היום, חיוני שמתקני התעשייה יגנו על המערכות האוטומטיות שלהם מפני התקפות סייבר אפשריות. שימוש בחומות אש, גיבויים והצפנת נתונים, עדכונים של תוכנה

וקושחה והתקנת תוכנת אנטי וירוס היכן שניתן – כל אלה דרכים שנועדו להגן על המתקן שלכם מפני התקפה.

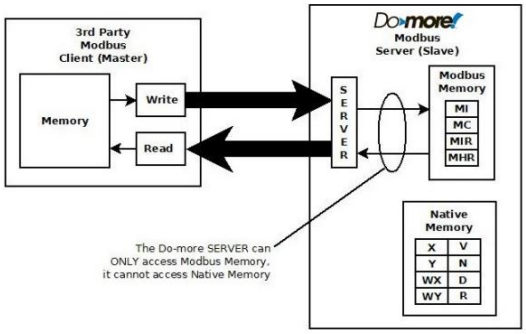
אך מה לגבי התקני הבקרה עצמם? בקרי PLC חדישים, דוגמת **Do-more! BRX**, מצוידים מראש באמצעי אבטחה מרובים ונועדו לסייע בהגנה מפני חדירות לא רצויות.

זיכרון אורח Guest memory

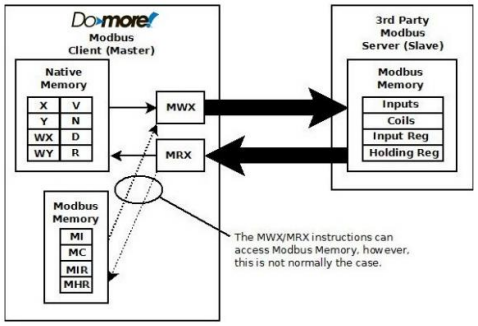
פלטפורמת **Do-more! BRX PLC** משריינת קבוצת בלוקים בזיכרון הפנימי במיוחד לצורך תקשורת חיצונית. בלוקים אלה מבודדים על מנת למנוע מהתקנים חיצוניים (כמו צגי מפעיל, HMIs, וכד') את היכולת לשלוט ישירות על התקני ה-I/O והזיכרון של הבקר. שיטה זו של תקשורת מגנה על הזיכרון המובנה (NATIVE) מפני גישה לא רצויה דרך ערוצי תקשורת.

בפועל, כאשר פלטפורמת **Do-more! BRX PLC** פועלת כשרת (Server) Modbus באמצעות Modbus/TCP או Modbus/RTU, היא מנתבת את בקשות הקריאה והכתיבה של Modbus מהתקנים חיצוניים אל ארבעת הבלוקים המבודדים בזיכרון ושמורים לתקשורת חיצונית. המידע המאוחסן בזיכרון האורח הזה יהיה זמין ונגיש לכל הוראת Ladder Logic.

בעת פעולה כלקוח (Client) Modbus, יוכלו פקודות **MRX** (Modbus Network Read) ופקודות **NWX** (Modbus Network Write) לגשת לכל זיכרון המובנה (native) וגם לזיכרון האורח עבור כל נתוני ההודעות היוצאות.



כתיבה/קריאה חיצוניים באמצעות הוראות ladder
עבור יישומי לקוח



כתיבה/קריאה חיצוניים באמצעות זיכרון אורח
עבור יישומי שרת

תקשורת מבוססת-הפעלה (Session-based)

בקרי **Do-more! BRX** רבים מותקנים ברשתות בעלות דרגות שונות של בידוד. דבר זה מאתגר מתכנתים ויצרני ציוד המעוניינים שהתקשורת עם הבקר תהיה מוגבלת לכוח אדם מורשה בלבד. לשם כך, תוכנת **Do-more Designer** משתמשת במדיניות של הפעלות התקשורת (Session) בכל פעם שהתוכנה נכנסת למצב מכוון מול הבקר.

לאחר שנוצרה הפעלת תקשורת, היא מקבלת זיהוי ייחודי. כל חבילת מידע (packets) חייבת לכלול את המזהה הזה. חבילה שתתקבל ללא המזהה הספציפי לא תטופל על ידי הבקר. בצורה זו תימנע גישה לא מורשית לבקר, וכן ימנעו מקרים שבהם מחשבים אחרים ברשת ניגשים בטעות לבקר הלא נכון. נעשה גם שימוש במערכת זמן קצוב שתסיים הפעלה לאחר פרק זמן ללא תקשורת בין התוכנה לבקר. במקרה כזה, יהיה צורך להפעיל/לפתח מחדש את ה- Session כדי שיתאפשר להמשיך בתקשורת מול הבקר.

הגנת כתיבה למערכת ההפעלה

לחיזוק והגנה על גרסאות קושחה (Firmware) של בקרי **BRX PLC,** כל בקר כולל 8 מתגי DIP בלוח האם, המשמשים לביצוע פעולות שונות של איתור באגים ושחזור. אחד מהמתגים מפעיל/משבית הורדות קושחה לבקר. השבתת הורדות קושחה תגן על הבקר מפני שינויים לא רצויים במערכת ההפעלה ותאפשר לכם לשמור על שליטה אם וכאשר שינויים כאלה יתבצעו.

סיסמאות/חשבונות משתמש ומעקב פעילות

מערכת האבטחה עושה יותר מאשר רק לאפשר או למנוע את היכולת להתחבר לבקר **Do-more! BRX** על בסיס זיהוי משתמש וסיסמה. אבטחת המערכת כוללת גם יצירת חשבונות שיאפשרו או ימנעו גישה למשאבים השונים בבקר. באמצעות יצירת חשבונות מרובים בעלי רמות גישה שונות, ניתן להגדיר ביעילות מי יקבל גישה לבקר ומה כל משתמש עם גישה יורשה לעשות. בעזרת חשבונות המשתמשים ניתן גם לעקוב אחר הפעולות שביצע כל חשבון. הודעות יומן האירועים יתעדו את חשבון המשתמש הפעיל עבור כל אירוע שנרשם, כך שתדעו בדיוק מי קיבל גישה ומתי.

פיתוחים בתחום התקשורת התעשייתית זימנו עד כה שיפורים רבים בתחום הבקרה המבוזרת, כולל תגובות מהירות יותר וגישה רחבה יותר. עם זאת, החידושים האלה גם פתחו את המגזר התעשייתי כיעד להאקרים פעילים ולארסנל ההולך וגדל של איומי הסייבר. משום כך, חשוב שתהיה יכולת לנטר את פעילות המשתמשים המורשים ואת הגישה הפיזית והמקוונת למערכת ולבקרים. קיימות דרכים רבות לשמור על המתקנים והרשתות מוגנים, וחלק מהבקרים וביניהם **Do-more! BRX**, יודעים להציע אמצעי הגנה מוכללים שיסייעו להדוף את חורשי הרעה. אנא השתמשו בתכונות אלו והגנו על המתקנים והמערכות בארגון.