איומים, יריבים ותרחישי תקיפה מרכזיים בעולם ה-OT

מאת גלעד זינגר

הקדמה

במאמרי הקודם ערכתי סקירת הכרות לעולם ה-OT, במה הוא שונה מהעולם המוכר של ה-IT, מהם רכיביו ומספר דוגמאות אודות שימושים נפוצים. במאמר זה ארצה לסקור מעט ממגוון האיומים, היריבים ומספר תרחישי תקיפה מסורתיים (רק כאלו שפורסמו בעבר על מנת לא לנטוע רעיונות בקרב יריבינו).

עלי לסייג כי קיים מגוון רחב של תחומים ומערכות אשר עושות שימוש ברכיבי בקרה החל מספינות, מבנים, מפעלים יצרניים לסוגיים, תעשיות אנרגיה (חשמל, גז) תעשיות המיים וכד', לכן אעסוק באיומים גנריים ולא כאלו המותאמים לתשתית כזו או אחרת.

במאמר הקודם ראינו כי רשימת הנכסים שונה בין שתי הרשתות וכך גם הטיפול באיומים וסיכונים כפי שלמשל בעולם מערכות המידע וה-IT השבתה למספר שעות אפשרית, בעולם התעשייתי הדבר לרוב בלתי אפשרי (קיימים מספר תאריכי השבתה חלקיים מוגדרים מראש). דוגמא אחרת לשוני בהתייחסות הינה כי התקני אבטחה מוכרים מעולם ה-IT לעיתים אינם מותקנים בשל החשש לשיבוש או מניעה של הפעלת תהליכים מרכזיים ברשת התפעולית.

ודבר אחרון לפני שנתחיל, המאמר מייצר סקירה תמציתית על מנת לאפשר לכם הקוראים **טעימה** בלבד מגורמי האיום בתחום זה ואינו מתעתד להחליף או לבוא במקום פרסומים ממשלתיים רשמיים.

מי היריב?

בדומה לעולם ה-IT, גם בעולם ה-OT (או בסביבת ICS- Industrial Control Systems) היריבים מגוונים ואף דומים בין העולמות. נתחיל בקווים לדמותו של היריב או מה למעשה עשוי להניע אותו.

בדומה לעולם ה-IT, הגורמים המניעים את היריב עשויים להיות מורכבים מהרצון לייצר שיבוש או סיכול של מערכות ICS או פגיעה בתהליך נקודתי (לעיתים ע"י שיבוש מידע) לטובת עיכוב או מניעה מטעמי תחרות, מלחמה/יריבות מדינתית, אנרכיזם או סתם עובד ממורמר.

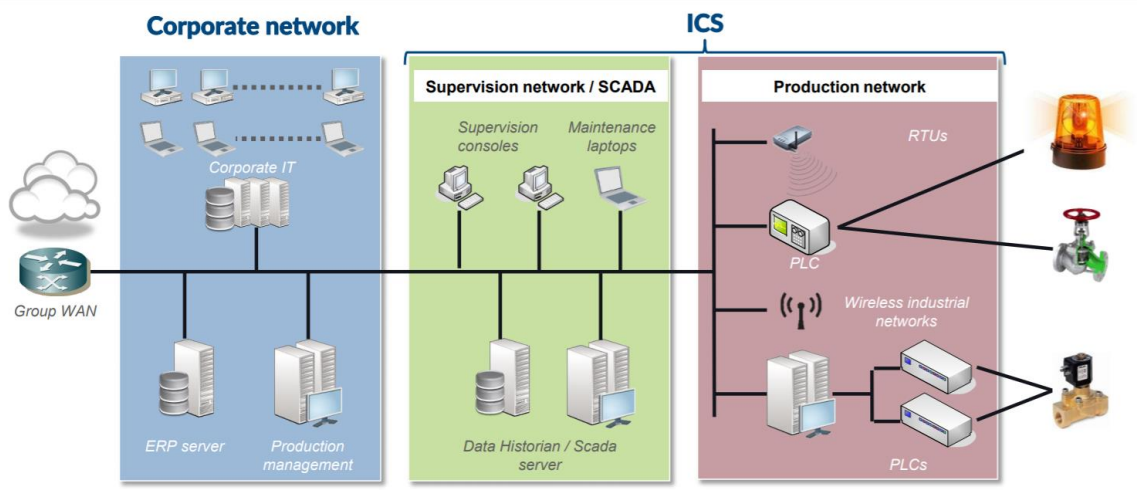
השגת רווח כספי - היריב (בין אם מדובר ביריב ישיר או מיקור חוץ) יבצע את פעולותיו במטרה לקבל תשלום עבור סיום ההתקפה, תיקון הנזק, שחרור כופרה וכד'. בשונה מעולם ה-IT, מרבית התקיפות לא יהיו במטרה להשיג מידע. נקודה זו משמעותית וחשובה שכן היא תשפיע על סוג ועוצמת הסיכונים וכן על מאמצי ההגנה אשר ננקוט במטרה להגן על נכסינו.

היריב יכול להיות עובד ממורמר שמעוניין לנקום על העדר קידום, חברה מתחרה המעוניינת ביתרון, ארגון פשיעה שבסה"כ רוצה הכנסה נוספת או כפי שדווח בשנים 2015-2016, יריבה מדינתית כדוגמת רוסיה אשר תקפה את אוקראינה ויצרה לראשונה הפסקת חשמל באמצעות תקיפה סייבר למעל 200,000 לקוחות במדינה.

התקיפה עשויה להיות מושתתת על מיקור חוץ של תשתיות תקיפה אזוריות שמטרתן לייצר השבתה, הרס או במקרים קלים יותר, ביצוע "ניסוי כלים" על מערכות חיות.

איומים מרכזיים על מערכות ICS

מי שקרא את המאמר הקודם, כבר מבין שמערכות ICS מקיפות אותנו בחיי היום יום. להבדיל ממערכות מידע בעולם ה-IT בהן מרבית האיומים הינם על המידע עצמו (סודיות, אמינות וזמינות), במערכות תעשיתיות האיומים משתנים בסדר העדיפות לזמינות ואמינות ורק לאחר מכן איום על סודיות המידע. בנוסף,איומים אלו עשויים להשפיע או לייצר תופעות לוואי שליליות כגון פגיעה בבטיחות ובתהליך הייצור. ניתן להחיל איומים שונים על חלקים שונים בתהליך וכדי שנבין זאת טוב יותר אתן תזכורת קטנה למבנה בסיסי של רשת תעשייתית.



את תפקיד הרכיבים בהרחבה ניתן לראות במאמר הקודם. מימין לשמאל נוכל להצביע על האיומים **המרכזיים** הבאים (כן... קיימים כאלו שלא אפרט במאמר):

סנסור או רכיב מפעיל (רכיב המקבל/שולח ערכים):

- פגיעה פיסית - חבלה פיסית ברכיב עצמו
- שיבוש/פגיעה בתעבורה - כתלות בסוג התעבורה מהרכיב (רדיו, סלולאר, קווי וכד')

בקר - שולט על פעילות הסנסור/מפעיל (מפעיל/מכבה, מושך נתונים וכד'):

- פגיעה פיזית ברכיב עצמו
- שינוי הלוגיקה הצרובה בבקר (מרחוק/קרוב - יפורט בהמשך)
- פגיעה בעדכוני תוכנה הניתנים להורדה לבקר
- שיבוש/פגיעה בתעבורת - כתלות בסוג התעבורה מהרכיב

שרת סקאדה המנהל את מערך הבקרים השונים:

- שיבוש/פגיעה בנתונים ובתהליכים התפעוליים
- שיבוש המידע אשר יוצג לבעלי עניין בתהליך התפעולי
- פגיעה בגיבוי תהליכים או במידע תפעולי

שרת היסטוריין המחזיק תעוד כלל הפעולות שבוצעו ברשת:

- שיבוש הנתונים הקיימים בשרת
- מניעת האפשרות לאחסן נתונים בשרת

עמדת צפייה ממנה ניתן לצפות בפעולות הבקר עליה תותקן תוכנת HMI (ממשק אדם מכונה):

- גישה בלתי מורשית (מרחוק/מקרוב - יפורט בהמשך) בשל העדר מדיניות אבטחת מידע (סיסמאות, פרופיל משתמש וכד')
- גישה למידע מסווג (עמדה זו תציג את שרשרת הערך של תהליך ספציפי ועשויה להיות מסווגת)

עמדת מהנדס ממנה ניתן (בין השאר) לייצר שינויים בבקר (שינוי לוגיקה או פעולות מיידיות):

- גישה בלתי מורשית (מרחוק/מקרוב - יפורט בהמשך) בשל עדר מדיניות אבטחת מידע (סיסמאות, פרופיל משתמש וכד')
- גישה למידע מסווג (עמדה זו תציג את כלל שרשרת הערך השל התהליך ועשויה להיות מסווגת)
- גישה לרכיבים נוספים במערכת (לדוגמא בקרים)
- הרכשה של גישות מרוחקות לעמדה (חיבורי VPN או חיבורים מרוחקים אחרים)

וכמובן בל נשכח שכלל הרכיבים מחוברים בסוגי תקשורת שונים (כולל תקשורת WAN/LAN, סריאלית, סלולארית או רדיו) ומעל הכל מרחפת לה עננת הרשת המנהלתית של הארגון המייצרת איום במידה וקיימת חיבוריות בינה לבין הרשת התפעולית.

תרחישים, ווקטורי תקיפה וסיכונים מרכזיים

קיים הבדל משמעותי בין מה שאנחנו רואים בסרטים לבין יכולות המציאות (מי ראה "מת לחיות 4"?), יחד עם זאת קיימים תרחישים לא פחות יצירתיים שידרשו מכם לפתוח את הראש ולהיכנס לראש של התוקף באשר הוא ומטרותיו.

כפי שציינתי בפרק הקודם אודות איומים, לא אסקור את כלל התרחישים המוכרים לכל אחד מהרכיבים ולמערכת בכללותה מכמה סיבות כאשר הראשונה שבהן היא לא לתת רעיונות זדוניים ל"מבקשי רעתנו" וכמובן כי תרחישים, איומים וסיכונים יכולים להיות מוכוונים "פר" מערכת - סיכון למערכת ICS במבנה חכם שונה מהסיכון למערכת בקו ייצור וכו' לכן בחרתי מספר תרחישים מרכזיים:

איום: שינוי לוגיקה בבקר
סיכון: החל משיבוש הפעילות התפעולית ועד לנזק לרכוש ואף פגיעה בחיי אדם
תרחישים רלוונטיים: טעינת לוגיקה בבקר יכולה להתבצע מקרוב ע"ב ממשק ייעודי (USB, סריאלי,כבל רשת ואחרים) או הורדת תוכנה לבקר מרחוק.

מתי נרצה לשנות לוגיקה לבקר? ראשית, כמובן לאחר בניית התהליך התפעולי הרצוי במתקן. פעילות הבקר תעבוד לרוב בצורה קבועה ולא משתנה - ניקח לדוגמא בקר האחראי על הדלקת תאורת רחוב כאשר החשיכה עולה ולכבות אותה לקראת הזריחה. סביר כי יעשה שימוש בסנסור אשר יקרא את כמות האור החיצוני, תהליך נוסף יבצע קריאה עיתית של נתונים מהבקר וכאשר הערך שווה לערך הצרוב בבקר, יופעל ריליי (מפסק) במערכת התאורה אשר יגרום להדלקתה (ולהיפך בכיבוי).

נניח ונרצה להוסיף תנאים נוספים לפעילות הבקר, למשל בעת שימוש בפאנל סולארי ייתכן ונרצה לשנות את הספק התאורה או להשפיע על זמני ההדלקה. לשם כך נרצה לבצע שינוי בלוגיקת הבקר.

טעינת הבקר מקרוב יכולה להתבצע ע"י בעל התפקיד המוסמך אבל כמובן ייתכן משתמש זדוני אשר נגיש לבקר פיסית ויוכל לבצע טעינה של לוגיקה חדשה לבקר.

תרחיש נוסף הינו חבלה בחבילת העדכון של הבקר באתר היצרן - מעת לעת מופצים עדכוני תוכנה לבקרים ע"י היצרנים. עדכונים אלו זמינים להורדה באתר היצרן. תוקף בעל גישה זדונית לאתר היצרן יכול להחליף את קובץ העדכון בקובץ "מטופל" ובכך לייצר נגישות לבקר ע"י טכנאי "משוטה", קרי עובד אשר חשב לתומו כי הוא מתקין את התוכנה העדכנית לבקר אך למעשה התקין קובץ זדוני בבקר אשר יאפשר לאחר מכן "טיפול" כזה או אחר בבקר.

ולסיום תרחיש הגישה המרוחקת לתכנות הבקר - ראינו כי במרבית התקיפות על מערכות ICS, שינוי בלוגיקת הבקר בוצע בדיוק בדרך זו ע"ב גישה מרוחקת למחשב מהנדס מערכת, לו הרשאת גישה לתכנות הבקר ומשם גישה ישירה לבקר ולשינוי לוגיקת הפעולה בו (ארחיב על כך בהמשך).

איום: שיבוש/מניעה של תעבורה באחד או יותר מרכיבי המערכת
סיכון: החל משיבוש הפעילות התפעולית ועד לנזק לרכוש ואף פגיעה בחיי אדם
תרחישים רלוונטיים: להזכירנו, קיימים סוגים שונים של בקרים ורכיבי מערכת ותצורות תקשורות רבות ומגוונות. מרבית התקשורת בין המערכות הקיימות כיום (בדגש על אלו שקיימות כבר שנים רבות ללא שדרוג) הינה גלויה לחלוטין. יתרה מכך, לא קיימים מנגנונים מובנים של אימות ואמינות המידע (Integrity) או ניטור בכל התהליך התפעולי.

גישה לא מורשית לתעבורה בכל אחד מצמתי המידע עשויה לאפשר לתוקף ציטוט והכרות של התהליכים ובשל העדר מנגוני אימות/אמינות/תקפות גם יכולת לבצע שידור מחדש. לתוקף קיימת אפשרות אף לשבש או לשלוח לרכיבים, פקודות לגיטימיות כביכול אבל כאלו שנוגדות את התהליך התפעולי.

לדוגמא בקר אשר אחראי על סגירת מגוף מים לאחר קבלת אינדיקציה מסנסור כי המיכל מלא. תוקף אשר יכיר ויהיה חשוף לתעבורת הבקר, יוכל לשנות את הפקודה ל"פתח" במקום "סגור" ולייצר במקרה הפשוט הצפה ובמקרה המורכב יותר הגלשה של שפכים, הזרמת חומרים מסוכנים וכד'.

איום: גישה לא מורשית לעמדת מהנדס
סיכון: החל משיבוש הפעילות התפעולית ועד לנזק לרכוש ואף פגיעה בחיי אדם
תרחישים רלוונטיים: מהנדס המפעל הינו דמות מרכזיות האחראית על התהליך התפעולי. עמדה זו תהיה בעלת הרשאות גורפות לרוב תהליכי המפעל, עמדה ניידת או נייחת (או גם וגם).

דרך עמדה זו המהנדס יכל לצפות בתהליכים ואף לשנותם בצורה רגעית או קבועה כגון לחיצה על מתג הפעלת המגוף או תכנות מחדש של הבקר באופן קבוע. השתלטות על עמדה זו תאפשר לתוקף נגישות ממשית לכמעט כל אחד מהאיומים שפורטו לעיל ולכן מדובר בעקב אכילס משמעותי בהסתכלותינו על רכיבי הרשת בהיבט אבטחת סייבר.

התרחיש המרכזי למימוש סיכון זה הוא תקיפת מחשב המהנדס או מחשב אחר ממנו המהנדס עושה שימוש לכניסה למערכת (לדוג' מחשבו הבייתי והלא מאובטח). לאחר תקיפת מחשב המהנדס ניתן יהיה ל"רכוש" את דרכי הגישה של המהנדס לרשת התפעולית ולרכיבי הרשת השונים.

דוגמא לכך הינה השגת גישה לVPN המאובטח של המהנדס לאחר תקיפת מחשבו או מחשב אחר ממנו עשה שימוש וניצול הרשאות החיבור לצרכי התוקף.

איום: גישה למידע מסווג (בטחונית/עסקית)

סיכון: חלק מתהליך איסוף המידע להרחבת התקיפה, פגיעה בסודיות המידע, פגיעה בתהליך התפעולי

תרחישים רלוונטיים: מידע מסווג ברשתות ICS יכול להיות לדוגמא כמות רכיבים כימיים, מידות ולוגיקות פעולה. לא נרצה שמידע זה יהיה נגיש ציבורית שכן חשיפתו עשויה לאפשר לתוקף השגת מידע נוסף להרחבת התקיפה ומידע אודות מה מיוצר במפעל, באיזו שיטה ומאפיינים נוספים שעשויים להוות סוד מסחרי (ואף סוד בטחוני במידה ומדובר בתעשייה צבאית).

תרחיש של השגת נגישות לאחד או יותר מרכיבי הרשת המחזיק באופן חלקי או מלא את המידע האמור, יאפשר חשיפתו ובמקרה החמור יותר שיבושו ע"י הכנסת נתונים שגויים אשר ייצרו שיבוש בתהליך התפעולי.

איום: חיבור בין רשת תפעולית לרשתות אחרות

סיכון: ווקטור כניסה למימוש תרחישי תקיפה נוספים

תרחישים רלוונטיים: החיבוריות או הקרבה בין רשת ה-IT לרשת ה-OT הינו הנושא המדובר ביותר בקרב גורמי אבטחה ובקרה בתחום ה-ICS ולא בכדי, מצד אחד החיבור הוא הכרחי לרוב בשל השפעת תהליכים תפעוליים על תהליכים עסקיים ולהיפך (כיצד תאגיד מים ידע כמה כסף לגבות באם לא ידע כמה הלקוח צרך?) ומהצד האחר, חיבור לא מאובטח עלול לייצר קישוריות של הרשת התפעולית הרגישה לרשתות אחרות מאובטחות פחות.

בעבר אמירה נפוצה היתה כי יש לייצר ניתוק מוחלט בין שתי הרשתות אך כיום ידוע וברור כי הדבר אינו אפשרי וגם באם היה, עדיין קיימות אפשרויות אחרות לתקיפת רשתות מבודדות לחלוטין.

התרחיש המרכזי הינו למעשה תקיפת רשת ה-IT שכאמור לרוב ציבורית יותר, מחוברת לאינטרנט ובעלת נגישויות רבות, ממנה יבצע התוקף גישה לרשת התפעולית וייצר נגישות לרכיבי הרשת השונים.

הערה - חשוב להכיר כי קיימים ספקים המחייבים שליטה מרחוק על רכיבים ברשת התפעולית כחלק מתמיכה כוללת ברשת ולכן בעת בניית תוכנית האבטחה עלינו לייצר מנגנונים מפצים לפערים אלו.

סיכום

עד כה סקרנו מהם עיקרי הנכסים - איומים - תרחישים - סיכונים במערכות ICS.

כפי שחשבתם, קיימים איומים מגוונים, חלקם זהים במהותם לאיומים על מערכות IT וחלקם חדשים ויחודיים למערכות OT. האיומים והסיכונים שהוצגו במאמר זה מבוססים על ארועי אמת שפורסמו בעבר ומטרתם כאמור הינה טעימה בלבד לעולם זה.

בשונה מעולם ה-IT, ניתן להגיד על סיכונים בעולם הOT כי הסיכון לחיי אדם הינו אמיתי ומשמעותי שכן מדובר במערכות קינטיות אשר מצד אחד עשויות לייצר פגיעה פיזית מיידית (זרוע של רובוט המשנה את צורת פעילותה וחובטת במפעיל) ופגיעה אוחרת (שינוי בתרכובת כימית של משקה). חלק ניכר מהאיומים והסיכונים על מערכות אלו הינו על בטיחות וזמינות המערכות ורק לאחר מכן לאלמנטים המוכרים לנו מאבטחת מידע לכן סביר כי תראו מחשבים ללא שומר מסך מוגן סיסמא במערכות ICS שכן קיים חשש כי בעת ארוע חירום, מחשב המפעיל ינעל ולא יהיה ניתן לתפעל את האירוע.

נכון, אפשר לצמצם את הסיכונים שהצגתי כאן ולייצר התערבות בתרחישי התקיפה. במאמר הבא אסקור שיטות ודרכים להתגוננות אם זה בהגנה אקטיבית, ניטור מערכות ואמצעים נוספים לצמצום הפערים המובנים.

לתגובות ועוד:

- linkedin.com/in/gilad-zinger
- twitter.com/GiladZinger