מבוא למערכות בקרה בעולם ה-OT

מאת גלעד זינגר

הקדמה

אנו רגילים לשמוע בכל מקום על אבטחת מידע וסייבר במערכות מידע, IT, אזורים פיננסיים, הגנה על אתרי אינטרנט, בסיסי נתונים הגנה על פרטיות וכד'. בנוסף, המילים: נתב, חומת אש ואפילו סוגי התקפות על מערכות כגון מניעת שרות, רוגלות ורושעות למיניהן, הפכו להיות שגרת השיח היומיומית בתקשורת.

אבטחת מידע "קלאסית" מושתתת לרוב על מודל ה-CIA - Confidentiality Integrity Availability ומתוך כך מרבית הנכסים עליהם נרצה להגן יהיו נכסי מידע (מוחשיים ולא מוחשיים) אשר הפגיעה בהם תוכל לייצר פגיעה בסודיות המידע, מהימנותו וזמינותו למשתמש.

הידעתם שיש יקום מקביל ל-IT בשם OT?

OT - Operation Technology - הינו התחום בו עולם הנכסים טיפה משתנה. מדובר ביקום בו חיים בקרים מתוכנתים, עמדות מהנדס ותפעול, שרתי סקאדה והמון הפתעות אשר למעשה משפיעות על כל מהלך בחיי היום יום שלנו לא פחות מעולם ה-IT.

ביקום זה עולם ה-**CIA** טיפה משתנה ונהפך ל-**AIC** שכן מדובר בתהליכים ופחות במידע. תהליכים בהם נרצה ראשית זמינות (לסגור את המשאבה מיד), מהימנות (מה הטמפרטורה האמיתית של מיכל אמוניה?) ולבסוף סודיות שכן לא נרצה לחשוף את תהליך העבודה של הבקר.

מאמר זה הינו ראשון מתוך סדרת מאמרים בה אפרט על הקווים לדמות עולם ה-OT, פרוט אשר יאפשר לכם הצצה קלה לעולם חדש-ישן זה. במאמרים הבאים נצלול לתחומי משנה בעולם ה-OT כגון עולם הבנייה (בנייה חכמה), מפעלים (Industry 4.0), עולם הספנות וכמובן נחבר את נושא ההגנה בסייבר בכל אחד מהתחומים.

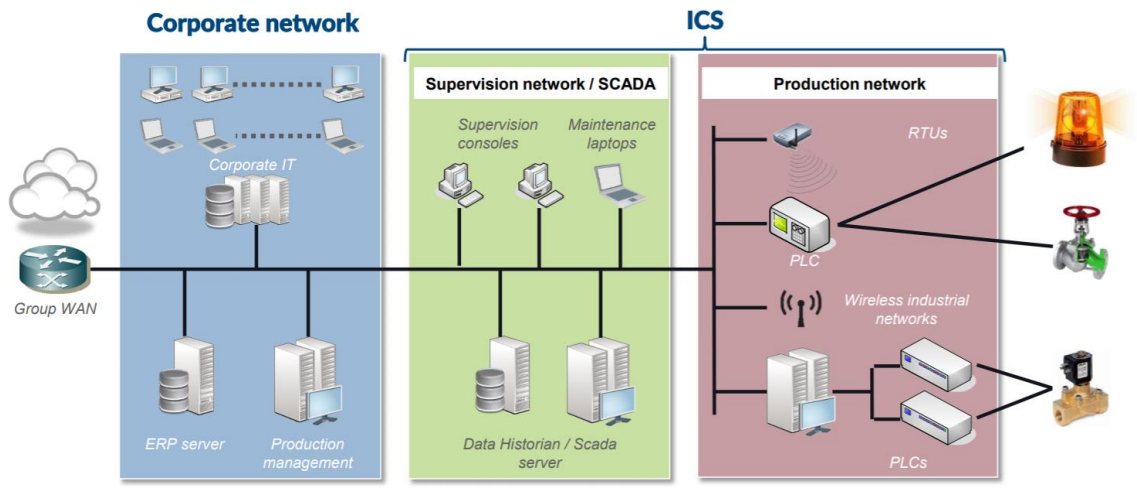
קריאה מהנה!

מבוא ל-ICS

נתחיל בקצת ראשי תיבות:

- Operation Technology - **OT**
- Industrial Control Systems - **ICS**
- Supervisory Control and Data Acquisition - **Scada**
- Distributed Control System - **DCS**

כיום אנשי מקצוע בתחום מתייחסים למערכות הללו לרוב בשם מערכות סקאדה. וכך היא נראת בכלליות:



מרכיבי המערכת (ארכז את המרכיבים המרכזיים בתחום):

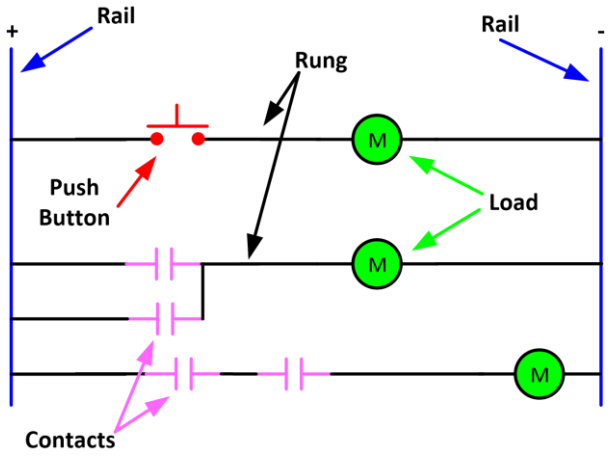
- **חיישנים/סנסורים/מפעילים:**

מאפשרים את החיבור בין עולם הבקרה לעולם הפיסי. חיישן יכול להיות לדוג' מדיד טמפרטורה אנלוגי או דיגיטלי אשר דוגם בזמן אמת טמפ' בחדר ומעבירה לרכיב הבא בשרשרת (בקר). מפעיל יכול להיות מנוע חשמלי או משאבה אשר מבצעת פעולה בהינתן פקודה (מהבקר...נכון). החיישן לרוב יעביר מידע לבקר והמפעיל בדיוק להיפך, יקבל מידע (1/0) אשר יפעיל או יפסיק את פעולתו.

- **בקר: Programmable Logic Controller - PLC**

מחשב זעיר בעל כניסות ויציאות (Inputs/Outputs) של מידע בינארי (לרוב). קיימים כרטיסי הרחבה לבקרים כולל עבודה רשתית ללא כניסה ויציאות ומגוון רחב של אפשרויות עליהם לא נדון בשלב זה. הבקר יתוכנת לרוב בלוגיקה קבועה מראש, אשר תאפשר פעילות ללא התערבות מפעיל בשגרה. הבקר יבנה לרוב מחומר עמיד וקשיח שכן קיימים מקרים בהם תידרש עמידות לטמפרטורות לא שגרתיות ולתנאים סביבתיים קשים.

לבקר תוכנה וחומרה אשר ניתנים לעדכון ושינוי. אחת משפות התכנות של הבקר הינה "דיאגרמת סולם", שפה המדמה את פעולת הבקר כפי שנוכל לראות בתרשים הבא:



דוגמא ללוגיקה שתיצרב בבקר: הפעלת מסוע במפעל בהינתן הגעת חבילה לאזור מסוים בו יעצור המסוע והחבילה תסומן ותיסגר [מה היה לנו כאן? מסוע שמקבל (INPUT), סנסור שמצביע על כך שהחבילה הגיע למקומה (OUTPUT), עצירת המסוע (INPUT)].

- **Engineering Station /Human Machine Interface - HMI**

עמדת שליטה ובקרה על הבקר, כתלות בהרשאות וסוג העמדה, היא תאפשר צפייה ב-FLOW העסקי של המערכת (מה מחובר למה תהליכית), צפייה בסנסור (לדוג' מהי הטמפרטורה, מה מפלס המים וכד'). בעמדות המוגדרות עמדות מהנדס או פיקוח, יהיה ניתן לבצע שינויים בבקר עצמו ואף לשנות את לוגיקת ההפעלה מרחוק או לבצע הפעלה או הפסקה ידנית של תהליכים.

לדוגמא, מקרה בו קיימת תקלה בבקר ועל המהנדס לבצע מעקף של פעילות קריטית בתהליך, תינתן האפשרות לבצע התערבות בתהליך בצורה ידנית ולכבות/להדליק רכיב פיזי מרחוק (למשל משאיבת מים). לרוב נוכל לראות עמודת HMI מותקנות עם מערכות הפעלה מסוג חלונות (גם כאלו שלא נתמכות כבר, עליהן נדבר בהמשך), כמו כן לעיתים ישלבו תחנות אלו אמצעי תקשורת נוספים מלבד רשת רגילה (חיבורי רדיו, חיבורי סריאליים וכד').

- **Data Historian - היסטוריין**

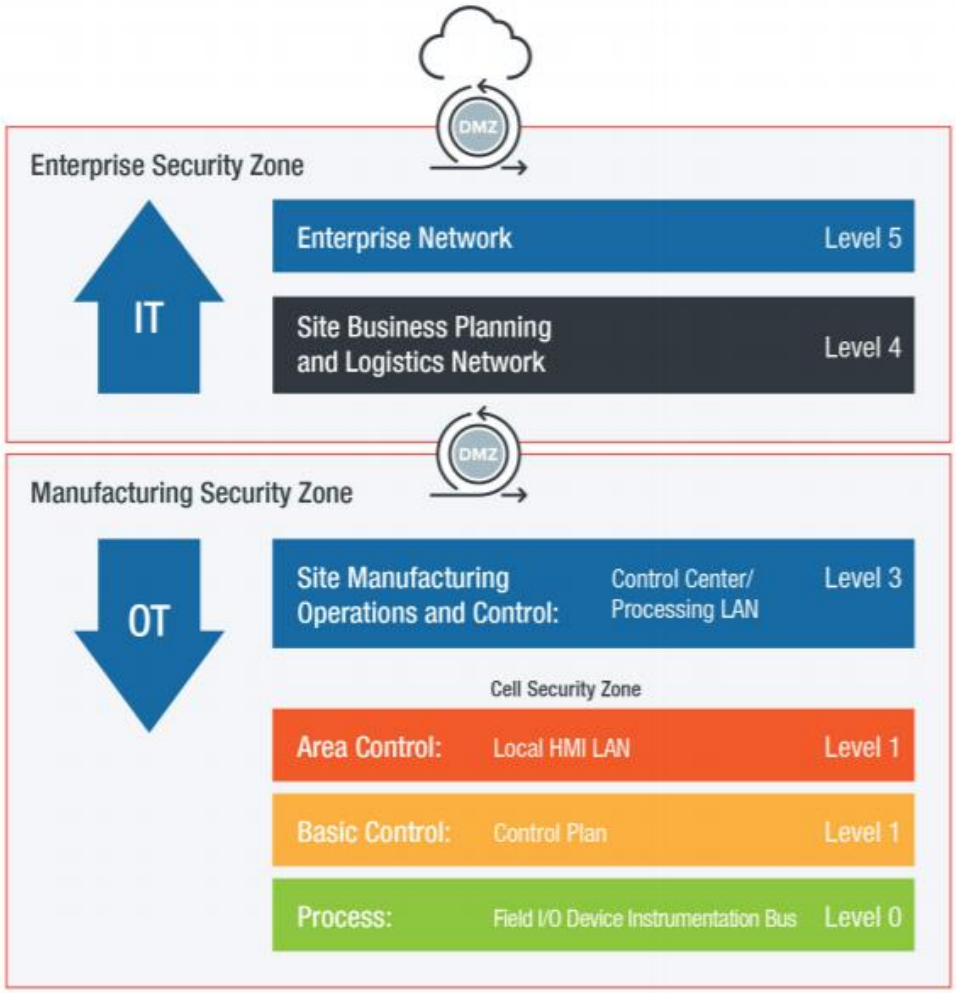
רכיב זה הינו למעשה בסיס נתונים האוגר כל פעילות המתרחשת ברשת ה-OT. הפעלת רכיב, קבלת חיווי מסנסור, טעינת קוד לבקר, עדכונים וכל פעולה אחרת, תנוטר ותועבר לשרת ההיסטוריין, משם תוכל להישלח כקובץ לוג למערכת SIEM או למרכז שליטה ובקרה (SOC) לטובת אגרגרציה וקורלציה עם נתונים אחרים על מנת לאתר בעיות תפעוליות, ניתוח אוחר וכמובן איתור אירועי אבטחת מידע ברשת.

אז כיצד כל היופי מתחבר לרשת?

פה נבצע הפרדה בין שני מושגים בתחום - רשת עסקית/מנהלתית ורשת תפעולית:

הרשת המנהלתית (IT) הינה הרשת בה מתנהל הארגון, בין אם זה מפעל מזון או תחנת כוח. ברשת זו נוכל למצוא את שרת הדוא"ל, שרת הקבצים, מערכות ERP, חיבור לדומיין מרכזי וכמובן לרוב חיבור לאינטרנט!

הרשת התפעולית (OT) כשמה כן היא, משמשת לתפעול התהליכים, בין אם מדובר בתהליכי ייצור תרופה בפס ייצור, תהליך הזרמת שפכים או העברת מים אליכם לברז בבית, בקצה כל פעילות כזו יושב בקר אשר מחליט - כן או לא.



כמו בעולם ה-IT גם כאן נעשה שימוש בפרוטוקולי תקשורת רבים ומגוונים.

חלקם ייעודיים למערכות או תעשיות ספציפיות, חלקם פרי פיתוח של יצרן וניתנים לשימוש רק במערכותיו וחלקם נפוצים במרבית המערכות הקיימות כיום.

שמות כגון **DNP**, **PROFIBUS**, **61850 IEC**, **BACNET** הינם רשימה חלקית ומצומצמת מאוד של פרוטוקולים בשימוש התעשייה.

אחד הפרוטוקולים הנפוצים ביותר הינו **MODBUS**, פרוטוקול סריאלי במקורו משנת 1979 אשר הוסב לעבודה בסביבת תקשורת IP/TCP.

מדובר בפרוטוקול בתצורת MASTER SLAVE, כאשר סוג הפעילות המועבר נקבע ע"ב מספר ידוע מראש (Function Code). הפרוטוקול מאפשר קריאה וכתיבה לבקר, התעבורה בו אינה מוצפנת ולא נדרשים כל אמצעי זיהוי ואימות.

מכיוון שעולם ה-OT וותיק, תחילה העבודה התקשורתית התבצעה ללא תצורת התקשורת המוכרת לכולנו היום אך עם ההתפתחות הטכנולוגית נולדו תוספות והרחבות לפרוטוקולים הקיימים על מנת שיוכלו לשלב ולהשתלב בתקשורות מודרניות, אחת מהן הינה ההרחבה לעולם ה-IP/TCP, הרחבה שאפשרה קישוריות לעולם החיצוני אבל לא תוכננה לעבודה מאובטחת במקור.

אז אם באבטחת סייבר עסקינן, כמה מילים על פערים באבטחת תשתיות OT.

מהם הפערים העיקריים באבטחת מערכות ICS/OT?

- חיבור בין רשתות - כאמור במערכות OT אנו צפויים לפגוש לפחות שתי רשתות שונות, רשת תפעולית ורשת מנהלתית. ברוב המקרים הרשת המנהלתית תחובר לאינטרנט (כמובן עם/בלי אבטחה ייעודית), אך מה קורה במקרים בהם קיים קישור ישיר בין הרשת התפעולית לרשת המנהלתית? תארו לכם מצב בו תוקף (ועל כך נרחיב בפרק הבא) "גולש" לבקר אשר אחראי על פעולת משאיבת מים של חברת אספקה, כמה נזק ניתן לייצר באותו רגע?
- ניהול עדכונים - קיים ויכוח אינסופי בתעשייה הבקרה, האם לעדכן או לא לעדכן את מערכת ההפעלה של הבקר, של רכיב ה- HMI או של כל רכיב אחר במערכת שכן עדכון או שינוי של מערכות אשר מחד בנות לעיתים 20 שנה ומאידך אחראיות על תהליכים רגישים של ייצור, עשוי לייצר פגיעה או השבתה העלולה לגרום לנזק כספי או אף פגיעה בחיי אדם. כתוצאה מכך נוכל לצפות למערכות לא עדכנית (Un Patched) ולעיתים קרובות לפגוש "דינוזאורים" בדמות חלונות XP ואף גרסאות ישנות יותר אשר אינן נתמכות ופגיעות ביותר.

- פרוטוקולים לא מאובטחים - הזכרתי את פרוטוקול MODBUS ככזה שאינו מוצפן בגרסתו הבסיסית והנפוצה, כמוהו קיימים פרוטוקולים רבים המעבירים את התעבורה בצורה גלויה וברורה, ללא מנגנוני הזדהות או אימות משתמשים וללא תמיכה בכל מערך אבטחה כזה או אחר המוכר לנו מעולם ה-IT.

- מודעות עובדים - איפה אתחיל? בעולם ה-IT מונהג בארגון המכבד את עצמו, תפקיד של CISO אשר אחראי על אבטחת המידע בארגון וחלק ממעגלי האבטחה הינה האדם עצמו (או העובד) לכן אנו רואים תהליכים רבים של העלאת מודעות העובדים לאבטחת מידע בארגונים רבים, גדולים כקטנים.

אך מה קורה בעולם ה-OT? כפי שהזכרתי בפתיח, לנכסי המידע קיימת חשיבות נמוכה יותר בעולם זה וברוב הארגונים לא תאתרו CISO אשר אמון על נכסי ה-OT מכאן שגם פחות נראה תהליכי מודעות עובדים או הכרות עם בעיות ההגנה בסייבר בעולם זה. עובדי תפעול אחראים שהתהליך בקצה יעבוד שכן כל עצירה של תהליך המפעל הינה אובדן כסף למפעל, האם במקרה כזה תמיד יבצעו חשיבה נוספת לפני שלמשל יחברו כרטיס סלולארי לבקר קריטי כדי לשפר את הקליטה שלו? לא חושב...

- ניהול מרוחק: מערכות הבקרה בעולם ה-OT מורכבות מאוד ולרוב נמכרות למפעל כמקשה אחת מהיצרן (או מיותר) כולל חבילת תמיכה מרחוק. תמיכה זו יכולה להתבטא בהשתלטות מרוחקת על בקר, עמדת מפעיל או כל רכיב אחר בתהליך המפעלי. בנוסף, קיימים ספקים (מחו"ל) אשר לא יאפשרו אחריות על המוצרים ללא פתיחת האפשרות לגישה מרחוקת לרכיבי המפעל בכל עת וללא אישור מבעוד מעוד. כמובן שפתיחת גישה מרחוק ללא הגבלה או שליטה, מאפשרת כר רחב לאפשרויות תקיפה של מערכת הבקרה דרך "שרשרת האספקה" (עליה יורחב במאמר הבא).
- בקרה- אנו מכירים היטב מעולם מערכות המידע תהליכי SOC/SIEM המאפשרים ניטור של רכיבי הרשת ומשתמשיה באופן כמעט הרמטי ומאפשרים קבלת התראות בזמן אמת אודות פרצות אפשריות, כניסות למערכת או תהליכים לא מורשים ולמעשה מסייעות ביצירת תהליך Incident Response ראוי במקרה של תקיפה או ניסיונות תקיפה והכלתה. בעולם ה-OT המצב קצת יותר מורכב בשל חוסר בשלות (קיימים ניצנים בתחום) הנובע בעיקרו מתפיסה שגויה של "אני מנותק מהעולם לכן אני מוגן". בשנים האחרונות אנו מתחילים לראות פתרונות ראויים בשוק אשר יסייעו לחבר את המפעל ותהליכיו למוקדי SOC (באתר או באתרים חיצוניים) תוך שמירה על אבטחת המידע (חזרנו למידע בדמות לוגי הרישום של המערכת).
- הכשרות - קיימות מעט מאוד הכשרות בתחום הגנה בסייבר של מערכות OT ואלו שקיימות מתקיימות בחול בלבד ועולות יותר משנה אקדמית (לקורס של חמישה ימים). כתוצאה מכך קשה לאתר גורמים בארץ הניתנים להגדרה כבעלי נסיון בתחום (אני בכוונה נמנע מהמילה "מומחה") וקיימים מקרים בהם ארגונים עשויים לקבל מענה אבטחתי המתאים לעולם ה-IT , לגורמי האיום והסיכונים הנלווים אליו ולא לאלו המתאימים לעולם ה-OT - וכן, הסיכונים שונים לחלוטין!
- תכנון ללא חשיבה אבטחתית - עולם הבקרה נולד שנים לפני עולם ה-WEB המוכר לכולנו. מדובר בתשתיות ורכיבים אשר לא תוכננו להתחבר לעולם החיצון, בעלי נגישות במערכות סגורות בלבד והחשיבה סביב תכנון לא כללה היבטי אבטחת מידע או הגנה בסייבר כלל שכן האיומים המוכרים לנו היום לא היו מוכרים או לחילופין לא היו רלוונטיים בעת תכנון מערכות הבקרה הוותיקות.

סיכום

מערכות ה-OT מלוות את חיינו לא פחות ממערכות הבנק או מערכות המידע אליהן אנו רגילים להתייחס בהיבטי אבטחת מידע. תהליכים תעשייתיים כוללים ייצור, בקרת תהליכים, ייצור חשמל, ייצור וזיקוק, הם עשויים להיות ציבוריים או פרטיים, והם כוללים טיפול במים והפצה, איסוף וטיפול בשפכים, צינורות נפט וגז, הולכה וחלוקה של חשמל המיוצר בתהליכים ושיטות שונות.

מדובר בשדות תעופה ואפילו אוניות וספנות, מעליות ומערכות מבנה, בהם נדרש לפקח ולשלוט על מערכות אקלים ומיזוג אוויר מערכות (HVAC) וצריכת אנרגיה. בתעשיות אלו נעשה שימוש יומיומי בתשתיות OT קריטיות אשר כל הפרעה לפעולתן עלולה לייצר תגובת שרשרת של פגיעה במוצר, פגיעה באספקה, שיבוש ועד פגיעה בנפש. כמעט בכולן יש בקר קטן בקצה המחליט האם המעלית תרד, האם חם מידי ויש לקרר, או האם פרצה שריפה ויש לקרוא באופן אוטומטי לכוחות הכיבוי.

אם הגעתם עד כאן, אתם יכולים כבר להבין כי המורכבות של התהליכים, נכסי ההגנה, האיומים והסיכונים בקצה, במרבית המקרים, שונים לחלוטין מעולם ה-IT וכל טעות או חדירה עלולה לייצר תגובה הרסנית.

אחד האתגרים המשמעותיים בתחום ה-OT, עליו אכתוב בהרחבה במאמר הבא, הינו אבטחת המערכות שכאמור לא תוכננו לכך מראש, עם "הפרעה" מינימלית לתהליכי יצור קריטיים ואפשור עבודה תקינה ורציפה לבעלי התפקידים הרלוונטיים.

אמינות מערכות SCADA בתשתית המודרנית שלנו עשויה להיות חיונית לביטחון ולבריאות הציבור. לפיכך, התקפות על מערכות אלו עשויות להיות קריטיות. תקיפה כזו כבר התרחשה, שבוצעה על מערכת בקרת שפכים של המועצה של מארוצ'י שייר בקווינס לנד, אוסטרליה. זמן קצר לאחר שהקבלן התקין מערכת SCADA בינואר 2000, רכיבי המערכת החלו לפעול באופן לא יציב. משאבות פעלו שלא צורך ומערכות ההתרעה לא פעלו באופן תקין. שפכים הציפו פארק סמוך וזיהמו תעלת ניקוז פתוחה של מי התהום. במערכת ה-SCADA כוונו שסתומי ביוב על פתיחה כאשר הפעולה המתוכננת הייתה אמורה לשמור אותם סגורים. בתחילה זה נראה כבאג במערכת אך מעקב אחר יומני המערכת גילה כי התקלות היו תוצאה של התקפות סייבר. החוקרים דיווחו על 46 מקרים נפרדים של התערבות חיצונית זדונית לפני שהאשם זוהה. ההתקפות בוצעו על ידי עובד לשעבר ממורמר של החברה אשר התקין את מערכת SCADA, תוך תקווה שישכרו את שרותיו כדי להגן על המערכת הפגועה.

חומר למחשבה בפעם הבאה שאתם פותחים את הברז והמים זורמים...

פרטים ליצירת קשר:

http://linkedin.com/in/gilad-zinger

http://twitter.com/GiladZinger