

# מערכות בקרה מתקדמות משלבות פתרונות לאבטחת מידע עבור תחנות כוח

דניאל ארנרייך, סימנס ישראל בע"מ

- מבנה סטנדרטי של בסיס הנתונים המיושם עבור מערכת הבקרה
- העברת נתונים אשר מתבצעת בשפת תקשורת סטנדרטית
- שילוב של מגוון רכיבי חומרה ותוכנה מגורמי חוץ (3rd party)



## פרוט סיוכונים צפויים

מערכות בקרה בתחנות כוח עלולות להוות מטרה לפגיעה מכוונת, וגם חשופות למגוון תקלות לא מכוונות כתוצאה מפעולה שגויה או רשלנית על ידי מפעילים ומהנדסי תחזוקה. אירועים אלה עלולים להחזיר ווירוס למערכת הבקרה או ליצור "ערוץ חשוף" שבאמצעותו ניתן לבצע חדירות מכוונות (וגם חוזרות) למערכת. תקלות אבטחת מידע מסוג זה עלולות לפגוע בחלק מהמערכת או בכל המערכת, וגם לגרום להשבתה ולהפסקת ייצור חשמל וקיצור לתעשייה. בנוסף לכך, תהליך הפסקת פעולה פתאומי (או יותר מהיר מהמותר), עלול לגרום לנזק ולקיצור חיי הטורבינות והגנראטור המייצרים חשמל. מפעילים של תחנות כוח (בעיקר פרטיות) חייבים לקחת זאת בחשבון, כי הפסקות פעולה לא מתוכננות עלולות לגרום לפגיעה בתדמית שלהם ולגרום לכך שלקוחותיהם לא יוכלו לסמוך על אספקה רצופה ואמינה. יחד עם זאת, בכפוף להסכמי אספקה עם לקוחותיהם, הפסקת פעולה לא מתוכננת עלולה להוביל גם לקנסות ופגיעה בחוזה.

## פתרונות לאבטחת מידע

פתרונות לאבטחת מידע עבור תחנות כוח חייבות לספק מענה הולם למגוון סוגי האיומים שנוצרים על ידי גורם פנים ארגוני, או תוקפים מחוץ לארגון וכן לאיומים המופעלים מרחוק. הפעלה של

## מבוא

חברות חשמל וספקים פרטיים של אנרגיה Independent Producers Power (IPP) בעולם, מודעים יותר ויותר לאתגרים הקשורים להבטחת פעולה אמינה של מערכות הבקרה (C&I) מהסיבות למודעות הגוברת הינן: התרחשות של אירועים ואיומים חדשים הקשורים לאבטחת המידע (Security Data), הופעה של פתרונות חדשים להגנה בפני התקפות דרך הרשת (Attack Cyber), הצורך לחבר את מערכת הבקרה לרשת תקשורת של הארגון וכמו כן הצורך בהתחברות מרחוק למטרת איסוף נתונים ותחזוקה של מערכת הבקרה. השילוב של מערכות הבקרה עם פתרונות לאבטחת מידע מאפשר פעולה אמינה יותר של תחנת הכוח ללא הפסקות שעלולות להיגרם עקב תקלה במערכת המחשוב.

מאמר זה מפרט את הנושאים שיש להתייחס אליהם טרם בחירת מערכת בקרה מסוג Industrial Control Systems (ICS) עבור תחנת כוח חדשה או החלפה במסגרת שדרוג של מערכת בקרה קיימת. מערכות בקרה מתקדמות חייבות לספק מענה הולם לאתגרים המפורטים לעיל, ולשלב מגוון פתרונות חומרה ותוכנה המיועדים למנוע חשיפה לסדרה של איומים מצד הגורמים הידועים שעלולים לבצע גישה למערכת ללא הרשאה.

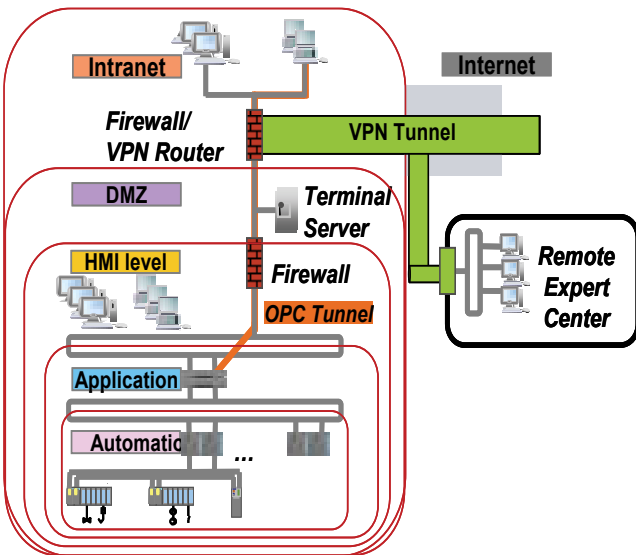
## מערכות מחשוב סטנדרטיות

מערכות תקשורת נתונים ומידע (Technology Information IT) ומערכות בקרה, מבוססות בדרך כלל על מחשוב סטנדרטי ומערכות הפעלה נפוצות בעיקר מסיבות של עלות נמוכה וזמינות ציוד חלופי. מצב זה יוצר סיכון בגלל שאנשי תחזוקה עלולים להשתמש בציוד מחשוב שהיה בשימוש קודם במקום אחר ובתפקיד שונה. מחשבים או שרתים אלה לא בהכרח מאובטחים כנדרש, ועקב כך הם עלולים להיות נגועים בוורוס (שנגרר מהתקנה קודמת) טרם התקנתם לצורך בקרה בתחנת כוח. להלן מספר דוגמאות שמבהירות את הנאמר:

- שימוש נפוץ במחשוב PC עם חומרה סטנדרטית לצורך בקרה
- שימוש של מערכת הפעלה מבוססת Windows Microsoft TM
- שימוש במגוון ממשקים סטנדרטיים: USB, IrDA, BLUETOOTH



- פעילותה של תחנת הכוח. לצורך השגת מטרות אלה, רשת תקשורת פנימית תופעל ע"פ חלוקה לאזורים, בכפוף לשיקולים הבאים:
- לאפשר שילוב של כל תת-המערכות בתחנת הכוח שנמצאות ברמה משותפת מבחינה של אבטחת מידע
  - לאפשר חיבור מאובטח בין חלקי המערכת אשר מבצעים את פעולות הבקרה לאותו המתקן ייצור.
  - לתכנן את מבנה המערכת כך שתהיה בה מספר מצומצם של נקודות גישה (חיבורים) מאזורים אחרים.
  - להפריד בין חלקי המערכות שאין להם צורך להיות מחוברים למתקנים אחרים (כגון חיבור בין תחנות כוח).
- הערה:** השיקולים המפורטים לעיל ישימים לכל סוגי החיבורים להעברת נתונים כולל רשתות עם חוטים וחיבורים אלחוטיים.



ציור 2 קישוריות לגורמי חוץ

### זרימת המידע בין המערכות

- מסיבות של אבטחת מידע, חשוב להבדיל בין נתונים שזורמים מכיוון מערכת הבקרה לגורם חיצוני (שנמצא באזור לא מאובטח) לבין זרימת נתונים מגורם חיצוני לתוך מערכת בקרה. דוגמאות לצרכים אלה הם:
- איסוף נתונים ממערכת הבקרה לצורך ביצוע שמירה וניתוחים עתידיים: Export of Operation Data (<--)
  - הצגה של תוצאות מחושבות וגם על גבי צגים הממוקמים מחוץ לתחנת הכוח: Offline Visualization (<--)
  - עדכון בסיס הנתונים, עדכון גרסאות תוכנה, וכן עדכון לצורך אבטחת המידע: SW and MPS Update (<--)
  - ביצוע אבחונים ותיקון של תקלות באמצעות גורם מקצועי חיצוני. Remote Service Access (<--)
- בתחנות כוח בהם נדרש לבצע איסוף נתונים והעברתם דרך רשת האינטרנט לגורם חוץ, מומלץ להעביר נתונים אלה דרך מערכת חד-כיוונית (Diode) עם סיב אופטי שבשום מקרה לא מאפשרת העברת נתונים לתוך המערכת.

אמצעים לאבטחת מידע חייבת להתבצע במקביל לתפקוד העיקרי של מערכת המחשוב: ביצוע בקרה אמינה ומתמדת על פעולתה של תחנת הכוח. אם משתמשים באמצעים לאבטחת מידע מספק חיצוני (rd party), אלה חייבים להיבדק בקפדנות רבה על מנת להבטיח כי שילובם לא יפגע בשום מקרה בפעולה תקינה ואמינה של מערכת הבקרה בתחנת הכוח.

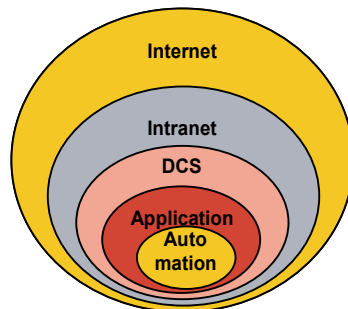
**הערה:** האמצעים שנבחרו לאבטחת מידע חייבים לקבל אישור מגורמים מוסמכים לנושא זה ולהיבדק באופן יסודי על מנת לוודא שאלה לא יגרמו להאטה של תהליכי המחשוב.

### פתרונות משולבים עם מערכת הבקרה

פתרונות אבטחת מידע עבור תחנות כוח מבוססים על העיקרון כי מערכת הבקרה חייבת להיות מאובטחת בעצמה. לכן, במצב זה כל שנדרש הוא להגן על מערכת הבקרה בפני איומים שעלולים לקרות כתוצאה מגישה למערכת הבקרה על ידי גורם פנים-ארגוני לא מורשה, או פריצה מכוונת מרחוק על ידי גורם חוץ.

הפתרונות המשולבים במערכת הבקרה חייבים לכלול את ההגנות הבאות:

- כל החיבורים הלא חיוניים כגון: רשת, חיבורי USB, כונני CD יפסיקו לפעול.
- תפעול הגנה נגד וירוסים שתתעדכן באופן קבוע: Malware Protection.
- אמצעי התקשורת האלחוטיים כגון: Wi-Fi, Bluetooth, IrDA יפסיקו לפעול.
- הסיסמה תופעל באופן מאובטח, על מנת להשיג אמינות אבטחה מרבית.
- תיבדק רשימת המורשים להפעלת המערכת ויבוצעו עדכונים תקופתיים.
- שימוש במבנה סיסמה מורכב, על מנת לחסום חדירה על ידי גורם זר.
- יבוטלו וימחקו כל היישומים במערכת ההפעלה שאינם חיוניים לצורך הבקרה.
- יתבצע רישום ממחושב של כל הכניסות למערכת על ידי משתמשים מורשים.



ציור 1 מערכת בקרה

### חלוקה לאזורי מידע מבודדים

מסיבות של אבטחת מידע, רצוי למזער את מספר החיבורים לרשתות החיצוניות. הקישוריות למשתמשים חיצוניים חייבות להבחן בקפידה על פי הצורך, ואם נדרש לאפשר חיבור כזה, ורק לפרק זמן קצר עד להשלמת הפעולה.

החלוקה לאזורי אבטחת מידע נועדה להגן על מערכת הבקרה מפני החדרת וירוסים והתפשטות שלהם לרוחב המערכת. כך ניתן להתגונן מפני מתקפה דרך הרשת (Cyber Attack) ולמנוע את השבתת

## מעבר דרך קישור DMZ

פתרון Zone Demilitarized (DMZ) הופך את החיבור בין האזורים לבלתי ישיר באמצעות מעבר דרך Server Terminal ושתי יחידות "חומת אש" כפי שמתואר בציור מס. 4, ובכך מאפשר לבצע בחינה יסודית של הנתונים המאושרים למעבר ולחסום נתונים שיש להם מבנה של וירוס.

פתרונות אלה מופעלים גם עבור מבנה מערכתי שבו שני אזורים ברמה דומה של צורך באבטחת מידע מחוברים זה לזה דרך רשת לא מאבטחת כגון רשת אינטרנט. פתרון זה מיישם את המבנה Virtual (VPN Network Private) אשר מספק חיבור מאובטח (PTP) Point to Point Secured, אבל בפועל התקשורת מתבצעת דרך רשת לא מאובטחת.

העברת נתונים מסוג זה נקראת "Tunneling VPN", כיוון שתהליך זה דומה למעבר דרך מנהרה שרואים מבחוץ אך פנים המנהרה לא נחשף.

מערכות בקרה מתקדמות עבור תחנות כוח חייבות לספק פתרונות אלה במסגרת חבילה לאבטחת מידע שכוללת:

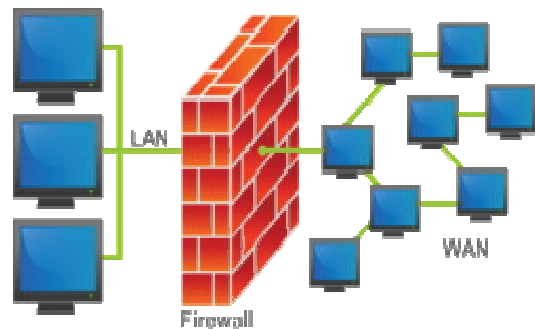
- הקשחה של כל החיבורים ובמיוחד אלה שלא חיוניים
- התקנה של אנטי וירוס שמתעדכן לעתים קרובות
- חיבור מאובטח לרשת התקשורת של הארגון
- תהליכי שמירת נתונים לצורך ניתוח עתידי ע"פ הנדרש
- חיבור מאובטח להתחברות מרחוק למטרת תחזוקה
- מגוון פתרונות נוספים כפי שמתוארים במאמר זה

**הערה:** לצורך התחברות מרחוק, יש לבחור בין חיבור דרך רשת המידע של הארגון או לבחור במסלול עצמאי.

## ישום "חומת אש" - Firewall

במערכות תקשורת נתונים ((IT משתמשים בפתרונות לאבטחת מידע והגנה מפני פריצות, שמטרתם לבצע סינון של התעבורה בין הרשת הפנימית לבין רשת החיצונית. ההבדל בין שני האזורים הוא ברמת הצורך באבטחת מידע.

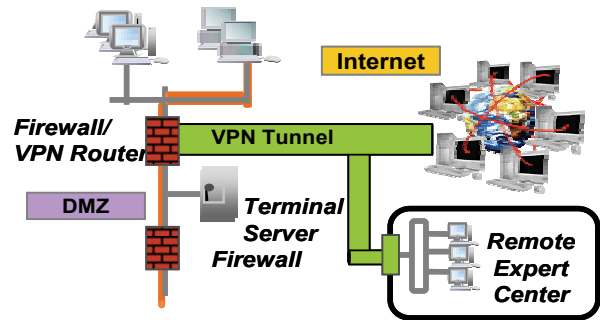
על מנת להיענות לדרישה זו, במערכות בקרה מתקדמות כל נקודת חיבור למערכת מאובטחת באמצעות חומת אש כמתואר בציור מס. 3. המגבלה הידועה של מערכות חומת אש (Firewall) כפי שמתוארת לעיל היא בכך שמבנה מערכתי זה מאפשר מעבר של נתונים מסוננים בין אזור מאובטח לאזור לא מאובטח.



ציור מס. 3. חומת אש

IDS. היתרון של פתרון זה הוא בכך שניתן להתאים אותו לכל מערכת. לעומת זאת החיסרון הוא בכך שהגילוי מתבצע לאחר שכבר החדירה החלה.

- מערכת גילוי המשלבת חדירה דרך הרשת וגם גישה ישירה למחשבים - IDS Based Hybrid. פתרון זה ניתן להתאמה מושלמת, בגלל שעלול לגרום לעומס מזערי בלבד ולא ישפיע לרעה על הביצועים של המערכת.
- מספר חברות בארץ ובח"ל שכבר זיהו את ההזדמנות, פיתחו מוצרים קטנים וקומפקטיים (Taps) שדוגמים ומקליטים את התעבורה ומאבחנים תשדורות חריגות. בעת בחירת מוצרים אלה, חשוב לבדוק ולאשר שפתרונות אלה לא יפגעו בביצועי המערכת.



ציור מס. 4 מימוש פתרון DMZ

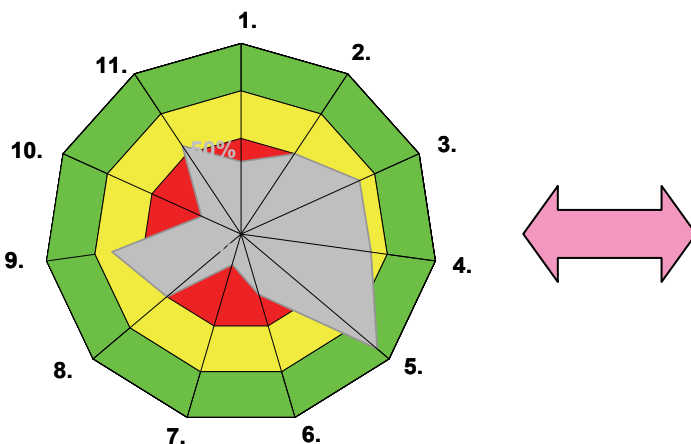
### עדכוני תוכנה ע"י התחברות מרחוק

התחברות מרחוק למערכת הבקרה נדרשת בדרך כלל למטרת של תחזוקה ולצורך הפצה של עדכונים (Patch Security Management). התחברות זו חייבת להתבצע באופן מאובטח כדי שלא תקרה תקלה כלשהי שעלולה להשבית את פעילות תחנת הכוח. בנוסף יש להתייחס לפעולות הבאות:

- עדכון תוכנה שנועדה להגן על המערכת בפני וירוסים Malware System Protection (MPS).
- סריקה תקופתית של מערכת ההפעלה והורדה של התקנות תוכנה לא חיוניות או פגומות.
- אבחון תקלות מערכת ומתן סיועה מרחוק לאיש תחזוקה מקומי המזהה בעיה שפתרונה דורש תמיכה חיצונית.
- הספק של מערכת הבקרה מחויב לתת מענה מתאים לצרכים אלו ולאפשר ביצוע התחברות למערכת הבקרה של תחנת הכוח מהמרכז בו יושבים מומחים לצורך תמיכה טכנית (Center Expert Remote). חבילות התוכנה והעדכונים המסופקים ע"י מרכז זה חייבות להיות בדוקות ומעודכנות.

### מערכת לבקרת תוכנות מאושרות

ידוע כי מערכות מחשוב רגישות לעומס הנגרם על ידי תוכנות הפועלות בו זמנית במערכת (בעיקר כאלה שלא חיוניות), ואלו עלולות לגרום



ציור מס 5 אבחון של האמצעים לאבטחת מידע

**הערה:** חשוב לציין כי במהלך תכנות אופן הפעולה של המערכת (system configuration), ובמהלך הפעלת המערכת (system commissioning) חייבים לבחון באופן קפדני שלא נשארו "פרצות" במערכת, שדרכם ניתן להגיע לאזור המאובטח. אמצעים אלה כוללים בין היתר גם בדיקה של המשתמשים ושימוש בסיסמה מורכבת.

### מערכות גילוי חדירה

הנושא של אבטחת מידע בעולם זוכה לתשומת לב רבה בעיקר עקב התגברות של פעילות עוינת שמטרתה לפגוע בתשתיות חיוניות באמצעות גישה דרך האינטרנט ופריצה למערכת הבקרה. מערכות גילוי חדירה (Intrusion Detection Systems) (IDS) למערכות בקרה ורשתות IT פועלות במקביל לפתרונות אבטחת מידע ונועדו לגלות ניסיונות פריצה למערכת באמצעות בחינה של הנתונים המועברים דרך אמצעי אבטחה כגון: Firewall, DMZ. פעולה זו מתבצעת באמצעות בחינה מעמיקה של הנתונים (ע"י יחידה עצמאית) וזיהוי של הפריצה אפשרית ע"פ סממנים ידועים. ישנן מספר אפשרויות מימוש תהליכים אלה:

- מערכת גילוי חדירה באמצעות החיבור לרשת - Based Network IDS. היתרון של פתרון זה הוא בכך שמאפשר לאתר את החדירה מייד בהתחלה. כמובן שתהליך זה דורש לבדוק כמות גדולה של נתונים.
- מערכת גילוי חדירה ישירה למחשבים הראשיים - Based Host

1. קיום נוהלי אבטחת מידע בארגון.
2. הדרכת עובדים לגבי נוהלי אבטחת המידע.
3. הגדרה מדויקת לגבי הגישה לכל סוגי המידע.
4. שמירה על סודיות המידע ע"י כלל העובדים.
5. אבטחה פיזית על מתקנים מסווגים.
6. חסימה למניעת גישה לרשת בארגון.
7. מעקב כניסות למערכת ע"י משתמשים.
8. תחזוקה מאובטחת של המערכת ע"י חיבור מרחוק.
9. טיפול נאות ומתועד לגבי חריגות מהנוהל.
10. תרגול נוהלי חירום למקרה של גילוי פריצה.
11. הקפדה על כל נוהלי אבטחת המידע.

## סיכום ומסקנות

מערכות לאבטחת מידע וכלים למניעת פריצות למערכת הבקרה של תחנות כוח חייבים לכלול אמצעים יעילים ואמינים. חשוב להתייחס לאמצעים אלה בתשומת לב מרבית וכמובן ע"פ דירוג רמת יעילותם. אומדן לחישוב החזר ההשקעה בפתרונות אלה לא ניתן כמובן למדידה באופן ישיר, אך אם באמצעות מערכת זו הצלחנו למנוע אירוע אחד בלבד כתוצאה מבעיית אבטחת מידע, הרי בכך הצדקנו את העלות ואת המאמץ שיש צורך להשקיע ביישום פתרונות אלה.



**דניאל ארנוביץ** (B.Sc.) משמש בתפקיד מנהל מכירות בחברת סימנס ישראל בע"מ בתחום מערכות מחשוב ובקרה לתחנות כוח. דניאל הוא בעל ניסיון מקצועי של מעל 20 שנים בשיווק מגוון תחומי מערכות בקרה ופעיל בתחומי כתיבת מאמרים ומתן הרצאות בנושא הבקרה.

להאטה של מערכת הבקרה. הפתרון לבעיה זו מיושם באמצעות תוכנת הגנה בשם Listing White (\*) שמגדירה רשימת תוכנות ויישומים המאושרים לפעול במחשבים של מערכת הבקרה. חשוב להדגיש שפתרונות אלה הם פתרונות משלימים לאמצעים של הגנה בפני וירוסים. לעומת זאת יש תוכנות אחרות שמוגדרות ברשימת ה-Listing Black, ואלה אסורות להתקנה על מחשבים שנועדו לבצע בקרה בתחנת כוח או לכל מטרה דומה. האתגר לגבי שילוב פתרונות תוכנה מיצרנים עצמאיים (3<sup>rd</sup> party) הוא בכך שצריך להשקיע מאמץ רב על מנת לבדוק את ההתקנה ולוודא באופן מוחלט כי תוספת זו לא תיצור השפעה שלילית על תפקוד מערכת הבקרה.

## ישום של מגוון אמצעים

שילובם של פתרונות תוכנה וחומרה לאבטחת מידע מהווה חוליה חיונית אך לא היחידה להבטחת פעילות אמינה של תחנת הכוח. האתגר של הגנה מפני מגוון סוגי פריצות וחדירות וירוסים אינו פשוט כלל, וקשה להתחייב מראש שפתרון כלשהו ייתן מענה מוחלט. לאור מצב זה, לא ניתן להסתפק באמצעי יחיד, וחשוב להיעזר גם במגוון אמצעים ניהוליים כפי שמתוארים ומדורגים בדוגמה שמופיע בצירוף מס 5.