היחידה לחיזוי טכנולוגי חברתי באוניברסיטת תל אביב

מיפוי תשתיות והתקנים המופעלים מרחוק

דו"ח מספר 1 בפרויקט

אבטחת התקנים ותשתיות המופעלים מרחוק

מחקר זה מומן על ידי משרד המדע והטכנולוגיה

מס' מענק בקרן 3-9775

יוני 2014

ד"ר יואל רבן

מר אמיתי דן

תל-אביב 69978, טל: 03-6407572 :TEL פקס: 03-6407570 ,ISRAEL, FAX: TEL - AVIV 69978

תוכן עניינים

דו"ח זה מהווה חלק ממחקר "אבטחת התקנים ותשתיות המופעלים מרחוק" המבוצע באוניברסיטת תל אביב עבור משרד המדע. היחידה לחיזוי טכנולוגי וחברתי באוניברסיטת תל אביב מתמדת בנושא המדיניות הכוללת של אבטחה התקנים ותשתיות המופעלים מרחוק בפני התקפות סייבר. דו"ח זה עוסק במיפוי ראשוני של טכנולוגיות להפעלת התקנים ותשתיות מרחוק ורשתות בקרה תעשייתיות וכן של תשתיות בהן מוטמעות הטכנולוגיות הללו (כולל תשתיות קריטיות). הדו"חות הבאים יעסקו בטכנולוגיות אבטחה של תשתיות והתקנים המופעלים מרחוק ובמדיניות אבטחה.

אנו רוצים להודות למר יניר לאובשטיין על הייעוץ והליווי של עבודת צוות היחידה לחיזוי טכנולוגי חברתי.

1. תקציר

1.1 דו"ח הנו חלק מעבודה הנעשית ע"י חוקרים מאוניברסיטת תל אביב ואשר מטרתה העיקרית הנה לסקור את הפגיעות של תשתיות והתקנים הנשלטים מרחוק במערכות בקרה תעשייתיות שונות, לספק פתרונות אבטחה חדשניים וכן לגבש המלצות למדיניות בנושא.

1.2 הדו"ח סוקר תשתיות וטכנולוגיות בקרה תעשייתיות קיימות, עומד על הפגיעות שלהן למתקפות סייבר, וכן מתאר בקצרה את מדיניות האבטחה של תשתיות רגישות בישראל ובמדינות אחרות. בדו"חות הבאים נסקור בפירוט יתר טכנולוגיות אבטחה נגד התקפות סייבר ונביא המלצות לשיפור מדיניות האבטחה בנושא זה.

1.3 רשתות (או מערכות) בקרה תעשייתיות הנן חלק אינטגראלי מן התשתית התעשייתית, והן כוללות מערכות בקרה מבוזרות (Distributed Control Systems), מערכות פיקוח, בקרה ואיסוף נתונים (SCADA), בקרים מתוכנתים (Programmable Logic Controllers), וכן התקנים כגון יחידות טלמטריה מרוחקות (Remote Telemetry Units), מדידים חכמים (smart meters), ושסתומים מתוכנתים מרחוק.

1.4 פרוטוקולים של רשתות תעשייתיות הם פרוטוקולים של תקשורת בזמן אמת אשר פותחו כדי לקשר בין מערכות, ממשקים והתקנים שיחד מהווים מערכת בקרה תעשייתית. נקודות החולשה של הרשתות התעשייתיות ידועות ברובן ונובעות ממחסור במודעות ובהנחיות ברורות, חולשות בקונפיגורציה של הפלטפורמה וכן חולשות של תוכנה, כגון מחסור בהגנה בפני נוזקות ומחסור בהצפנה.

1.5 יש דרכים שונות להתמודד עם הפגיעות של תשתיות ורשתות תעשייתיות והן באות לידי ביטוי בתקנים ובטכנולוגיות שונות. כך, למשל, ניתן להקים מובלעות (enclaves) הכוללות חלקים פונקציונאליים קריטיים ברשתות הללו ולהגן עליהם ב- firewall וכן ע"י התקני זיהוי ומניעת חדירות. תקנים בולטים בתחום הם תקני NERC CIP הצפון אמריקניים להגנה על האמינות של תשתיות חשמל קריטיות, תקני CFATS להגנה של מפעלים כימיים בפני טרור, וכן תקן ISO/IEC 27002:2005 של ISO ו- ANSI.

1.6 חלק מן התשתיות הרבות המופעלות מרחוק באמצעות רשתות בקרה תעשייתיות נחשבות כתשתיות קריטיות. יש מספר הגדרות של מהי תשתית קריטית. במספר מדינות הקריטיות מתבססת על היעוד של התשתית, במדינות אחרות ההגדרה מתבססת על ההשלכות של פגיעה בתשתית על החברה. באיחוד האירופי ההגדרה של תשתית קריטית היא נכסים או מערכות שהנם חיוניים לקיומם של פעילויות חברתיות כגון בריאות, ביטחון, וכלכלה. בארה"ב ההגדרה מתייחסת למערכות או נכסים (פיסיים או וירטואליים) שהם חיוניים עד כדי כך שפגיעה בהם תהיה בעלת השלכות גדולות על ביטחון בכלל וביטחון כלכלי בפרט, וכן על בריאות הציבור.

1.7 המחלקה לביטחון פנים בארה"ב מפרטת 18 סקטורים קריטיים, כגון אנרגיה, חקלאות ומזון, בנקאות ופיננסים, כימיקלים, תקשורת, ביטחון, וכן הלאה. ביפן רק 10 סקטורים ובבריטניה רק 9. בעתיד יכנסו יותר תחומים להגדרה של תשתית קריטית בגלל הגידול בחיבוריות (בתשתיות אינטרנט של עצמים, למשל) והמעבר למערכות תחבורה אוטונומיות.

1.8 ארגון ה- OECD סקר לא מכבר את מדיניות ואסטרטגיות הסייבר סקיוריטי של 10 מדינות OECD שונות. מדיניות להגנת מרחבי הסייבר ותשתיות קריטיות הקשורות אליהן נמצאת כבר בעדיפות לאומית גבוהה במדינות השונות. הדגש במדיניות הגנה מתרחב מהגנה על פרטים וארגונים להגנה על החברה כולה. כל האסטרטגיות שמות דגש חזק על הצורך של המדיניות לכבד זכויות בסיסיות כגון פרטיות, חופש ביטוי, וזרימה חופשית של מידע.

1.9 כבר ב- 2002 החליטה הממשלה לקבוע את האחריות להגנה על מערכות ממוחשבות בישראל, כולל הקמת ועדת היגוי שתבחן אלה גופים יוגדרו כחיוניים ולכן זקוקים להגנה קיברנטית אשר תסופק באמצעות יחידה ייעודית של השב"כ והיא הרשות לאבטחת מידע (רא"מ). הבסיס החוקי לאבטחה הקיברנטית בישראל מבוססת על החוק להסדרת הביטחון בגופים ציבוריים (התשנ"ח-1998) הקובע סמכות ואחריות לאבטחה פיסית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות של גופים ציבוריים.

1.10 מיזם לאומי להתמודדות עם האיום הקיברנטי (המטה הקיברנטי הלאומי) הוקם ב- 2010 על ידי הממשלה ותכנית העבודה שלו הוכנה ע"י פרופסור יצחק בן ישראל. המטה עוסק בהסדרה ותכלול הפעילות הכלל ממשלתית הנוגעת למרחב הקיברנטי בראייה אזרחית וביטחונית ולמעשה פועל לגיבוש מדיניות הגנה כוללת למרחב הקיברנטי.

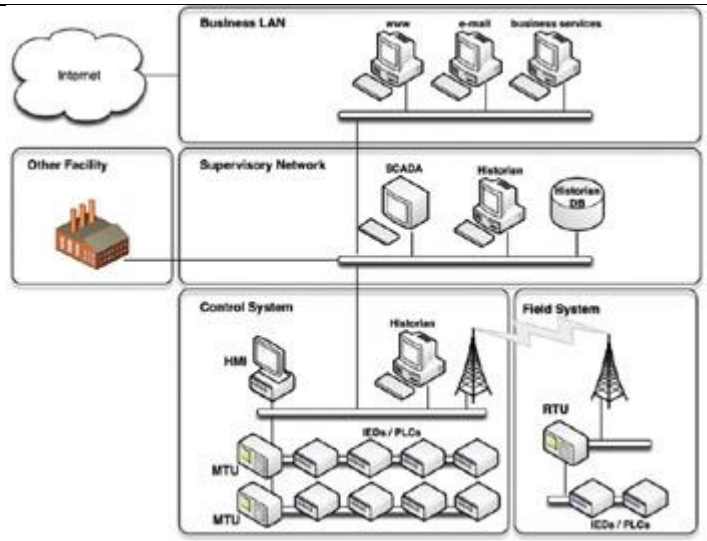
1.11 אל מול מתקני התשתית הפרטיים בישראל פועל משרד התשתיות הלאומיות האנרגיה והמים בכל הקשור להגנה ואבטחת מערכות המחשב החיוניות במתקנים אלו,זאת במסגרת אחריותו הרגולטורית. בעזרת נוהל שנכתב במשרד, מתקיים תהליך הכוונה ליווי והנחיה של מתקני תשתית פרטיים (לדוגמא במגזר הגז החשמל והמים) להגנה על מערכות המחשב החיוניות של מתקנים אלו.

2. מיפוי טכנולוגיות בקרה תעשייתיות[1]

2.1 רשתות תעשייתיות

רשת תעשייתית (industrial network) בנויה בדרך כלל ממספר מרכיבים – רשת עסקית, רשת תפעול עסקי, רשת פיקוח, ורשתות בקרה.רשת SCADA (Supervisory Control and Data Acquisition) הנה רק חלק ספציפי מרשתות הבקרה הללו.

רשתות (או מערכות) בקרה תעשייתיות הנן חלק אינטגרלי מן התשתית התעשייתית, והן כוללות מערכות בקרה מבוזרות (Distributed Control Systems), מערכות פיקוח, בקרה ואיסוף נתונים (SCADA), בקרים מתוכנתים (Programmable Logic Controllers), וכן התקנים כגון יחידות טלמטריה מרוחקות (Remote Telemetry Units), מדידים חכמים (smart meters), ושסתומים מתוכנתים מרחוק.



תרשים 2.1.1: רשת תעשייתית (מקור – Knapp)

מערכות תעשייתיות רבות מבוססות על מערכות מורשת (legacy) שקושרו במשך הזמן לרשתות מודרניות כגון רשת האינטרנט. לפני עידן האינטרנט תשתיות אנרגיה (לדוגמה) נבנו כדי לספק אמינות. הייתה דאגה לבטיחות פיסית אך לא התייחסו לאבטחת מידע, מכיוון שמערכות הבקרה היו מופרדות פיסית מן התשתיות. רשת הפיקוח הייתה מקבלת מידע מן הבקרה באופן חד כיווני ולא היה קישור בכיוון השני. הצורך במידע בזמן אמיתי גרם לכך שהחלה זרימת מידע דו-כיוונית וההפרדה הפיסית נעלמה, דבר אשר יצר סיכונים ממשיים של פריצה וחבלה במשאבים קריטיים.

[1] מבוסס במידה רבה על Eric Knapp, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA' and other Industrial Control Systems, Syngress Publishing 2011

בשנת 2010 יועצי אבטחה מחברת Red Tiger Security הציגו ממצאים של ניסיונות חדירה לכ- 100 מתקני ייצור אנרגיה בצפון אמריקה בהם התגלו 38,000 אזהרות אבטחה ופרצות. חברת הייעוץ גילתה גם שיש פער גדול מאד בין האזהרה בדבר פרצת אבטחה לבין ההתייחסות אליה במערכת הבקרה התעשייתית, דבר שנותן אפשרות להאקרים ופושעי סייבר לחדור לתוך רשתות בקרה ולהשתלט על מערכות תעשייתיות.

2.2 פרוטוקולים של רשתות תעשייתיות

פרוטוקולים של רשתות תעשייתיות הם פרוטוקולים של תקשורת בזמן אמת אשר פותחו כדי לקשר בין מערכות, ממשקים והתקנים שיחד מהווים מערכת בקרה תעשייתית. רובם תוכננו בתחילה לתקשורת טורית על חיבורים טוריים אבל הותאמו גם לעבודה על רשתות אתרנט תוך שימוש בפרוטוקולים של ניתוב כגון TCP/IP.

הפרוטוקול הוותיק ביותר והשכיח ביותר לתקשורת בקרה תעשייתית הוא **Modbus** (Modicon Communication Bus). זהו פרוטוקול בשכבת היישום של OSI, המאפשר תקשורת בין נכסים מקושרים המבוססת על מתודולוגיה של בקשה/מענה (request/reply). לכל התקן המתקשר באמצעות הפרוטוקול חייבת להיות כתובת ספציפית, כך שרק ההתקן שאליו מיועדת הבקשה יוכל להגיב. התקשורת מתחילה בהעברת קוד ובקשה וההתקן המקבל מגיב עם הקוד וכן עם מענה, אם אין שגיאות.

ניתן לבצע מספר פקודות באמצעות הפרוטוקול, כגון בקרה של ממשק קלט פלט, קריאה ממשק קלט פלט, קריאת ערך ברג'יסטר, כתיבת ערך לרג'יסטר. הפרוטוקול מותקן בדרך כלל בין בקר מתוכנת לממשק משתמש, או בין בקר מתוכנת לבין slave devices שהם בקרים מתוכנתים, ממשקי מחשב, חיישנים, אמצעי קלט פלט, וכן הלאה. בעיות הבטיחות העיקריות של פרוטוקול ה- Modbus הן חוסר אותנטיקציה (התקשורת מצריכה רק כתובת וקוד אותם ניתן לנחש או להשיג בנקל), חוסר הצפנה (ניתן להעתיק פקודות וכתובות), חוסר של checksum (ב- Modbus TCP), ויכולת תכנות שהיא התכונה המסוכנת ביותר המאפשרת החדרת קוד זדוני לבקר מתוכנת או ליחידת טלמטריה מרוחקת. רצוי להשתמש בפרוטוקול רק לתקשורת בין התקנים ידועים תוך שימוש בקודים צפויים שניתן לנטר בקלות וליצור מובלעת ברורה והתנהגות מקובלת.

פרוטוקול נוסף הוא **ICCP** (Inter Control Center Protocol) שתוכנן לתקשורת בין מרכזי בקרה בתעשיית האנרגיה. הפרוטוקול מבצע מספר פונקציות תקשורת בין מרכזי בקרה, כולל יצירת קישור, גישה למידע, העברת מידע, העברת הודעות, קונפיגורציה של התקנים מרוחקים, בקרה של התקנים מרוחקים ובקרה של תוכניות ביצוע. הפרוטוקול מגדיר תקשורת בין שני מרכזים במודל שרת-לקוח, כאשר מרכז אחד שהוא השרת כולל נתוני יישומים ופונקציות מוגדרות, והמרכז השני שהנו הלקוח מוציא בקשות לקרוא מתוך השרת. הפרוטוקול מיושם בדרך כלל תוך שימוש ב- ISO transport על פורט TCP 102 תוך שימוש בלוח בילטרלי המגדיר הסכמה בין שני מרכזי בקרה. הפרוטוקול סובל

מכמה בעיות אבטחה כולל חוסר אותנטיקציה והצפנה, הגדרות מפורשות של יחסי אמון ושימוש בלוחות בילטראליים, וכן נגישות גבוהה המושכת מתקפות כולל DoS. קיימת גרסה מאובטחת של ICCP הכוללת אותנטיקציה באמצעות digital certificate והצפנה.

פרוטוקול **DNP3** החל את דרכו כפרוטוקול טורי המתוכנן לשימוש בין תחנות בקרה שהן master לבין התקנים שהם slaves. הפרוטוקול הורחב לשימוש מעל IP כדי להקל בתקשורת עם יחידות טרמינל מרוחקות. בניגוד לפרוטוקולים הקודמים DNP3 הנו גם דו-כיווני והוא מאפשר לתחנת קצה לדווח ל-master על מאורע מעבר לאינטרוול הדגימה הנורמאלי. המטרה העיקרית של הפרוטוקול היא לשלוח ולקבל הודעות בין התקנים של מערכת בקרה. תקשורת ראשונית כוללת בקשה מהמסטר לתחנת קצה לקרוא נתונים לתוך בסיס הנתונים במסטר. תקשורת נוספות יהיו לצורך דגימה ישירה או בקשה ספציפית, תגובה יזומה של תחנת הקצה, או בקשת בקרה או קונפיגורציה מהמסטר ליחידת טלמטריה מרוחקת. קיימת גם גרסה של DNP3 מאובטח הכולל אותנתיקציה לתהליך השאלה/תגובה.

2.3 רשתות תעשייתיות בפעולה

יש מספר התקנים בהם נעשה שימוש ברשתות תעשייתיות, כולל התקנים תפעוליים (חיישנים, מנועים, מגופים) והתקנים אלקטרוניים חכמים אחרים, יחידות קצה מרוחקות (RTUs), בקרים מתוכנתים (PLCs), ממשקי משתמש (HMI), נכסי מערכות בקרה, תחנות עבודה של ניהול הפיקוח, וכן קונסולות של מידע עסקי.

התקן אלקטרוני חכם (Intelligent Electronic Device – IED) הוא התקן המהווה חלק ממערכת בקרה, כגון חיישן, מפעיל (actuator), מנוע, שנאי, משאבה, המצויד במעבד זעיר שמאפשר לו לתקשר באופן דיגיטאלי. התקנים אלה מתקשרים בדרך כלל באמצעות פרוטוקול fieldbus[2] ומתפקדים כצמתי עבד (slave) ומבוקרים באמצעות יחידת קצה מרוחקת או בקר מתוכנת.

יחידות קצה מרוחקות (RTUs) נמצאות בדרך כלל באתר מרוחק והן מנטרות פרמטרים מסוימים ומעבירות נתונים לתחנת ניטור מרכזית, ליחידת קצה המתפקדת כאדון (master) או לבקר מתוכנת הממוקם במרכז המערכת, או ישירות לממשק משתמש. יחידות קצה מרוחקות כוללות יכולות תקשורת כגון מודם, קישור סלולארי, רדיו, או רשת WAN. הן עושות שימוש בדרך כלל בפרוטוקול DNP3 לתקשורת בין אדון ליחידות מרוחקות, וב- DNP3 או Modbus לתקשורת עם התקנים אלקטרוניים חכמים.

בקרים מתוכנתים (PLCs) הנם מחשבים ייחודיים שנועדו להפוך פונקציות שונות ברשתות תעשייתיות לאוטומאטיות. אלו הם התקנים מוקשחים שנועדו לשימושים ספציפיים ואשר תוכנתו להגיב אוטומאטית לתשומות מסוימות (מחיישנים למשל) עם תקורה מינימאלית. התקנים אלה בדרך

[2] http://en.wikipedia.org/wiki/Fieldbus

כלל מבצעים בקרה של תהליכים בזמן אמת, כגון בקרת חום בתנור אפייה, בקרת רמזורים, בקרת השקיה, וכדומה.

ממשק אדם מכונה (HMIs) נבנה כדי לאפשר למתפעל המערכת גישה נוחה להתקנים השונים והוא מחליף מתגים ובקרות ידניות שהיו נהוגות בעבר. הממשקים הללו מאפשרים התחלה ועצירה של מחזורים, וכן פעולות אחרות הנדרשות כדי לבצע התאמות ואינטראקציה עם תהליך הבקרה.

תחנות עבודה מפקחות (Supervisory Workstations) אוספות מידע מנכסים שהנם חלק מרשת תעשייתית ומציגות אותו לצורכי פיקוח. מן התחנות הללו, בניגוד לממשק משתמש, ניתן רק לקרוא נתונים. תחנה כזו יכולה להיות בנויה ממשק משתמש (רק לקריאת נתונים) או מאוגר נתונים (data historian) שנועד ספציפית לבצע ביקורת של מערכת בקרה.

רשתות תעשייתיות הנן דרך כלל מאד מפוזרות ובעלות טופולוגיות שונות, בהשוואה לרשתות עסקיות . רשתות SCADA ורשתות בקרה תעשייתית יכולות להשתמש בטופולוגיות bus, ring, star או tree, מותנה בסוג תהליכי הבקרה ובפרוטוקולים בהם נעשה שימוש. ה- DMZ SCADA צריכה לתקשר עם מספר פרוטוקולים של רשתות תעשייתיות ומצד שני עם רשתות אתרנט TCP/IP מפעליות.

רשתות הבקרה התעשייתית נועדו כדי ליצור אוטומאציה של פעילות תעשייתית כלשהיא, כגון זיקוק נפט, סינון מים, יצור חשמל, וכן הלאה. רשת תעשייתית טיפוסית כוללת בדרך כלל מספר שכבות של לוגיקה מתוכנתת שנועדה לתפעל בקרות מכאניות לצורך אוטומאציה של ההליך התעשייתי. כל פונקציה ייעודית הופכת לאוטומאטית על ידי **לולאת בקרה** (control loop). לולאה כזו נוצרת ע"י התקן בקרה, למשל PLC, עם תכנות מסוים, שמבצע פעולה חוזרת שהופכת פונקציה תעשייתית נתונה לאוטומאטית. למשל, מחמם מים מתוכנת להביא את הטמפרטורה של המים ל- 90 מעלות ואז מופעל מפסק. לולאות בקרה יכולות להיות פשוטות כמו הדוגמה הקודמת, או מורכבות או מרובות שמבצעות בקרה על מספר תהליכים במקביל.

תהליכי בקרה מגדירים חלק גדול יותר בתפעול תעשייתי. הרבה תהליכים תעשייתיים נדרשים כדי לייצר מוצר או לייצר חשמל. תהליך אחד, לדוגמה, יכול להיות להזריק חומר מסוים לתוך מיקסר, והתהליך לכשעצמו מורכב מלולאת בקרה שפותחת שסתום בתגובה למדידות נפח וטמפרטורה בתוך המיקסר. כל תהליך כזה מנוהל על ידי ממשק משתמש שמספק תמונה (קריאה) של התהליך מאחת או כמה לולאות בקרה. כל תהליך מסתמך על משוב כלשהו בתוך לולאת בקרה ובין לולאת בקרה לממשק משתמש. משוב (לולאות משוב) ניתן בדרך כלל ממשק המשתמש, אך ניתן גם לרכז אותו על פני תהליכים מרובים. ניהול מידע מרוכז במערכת בקרה תעשייתית מבוצע בדרך כלל ע"י מערכות אוגרי נתונים (Data Historians) בתוך המערכות הללו או תוך שימוש בכלי ניתוח חיצוני כגון אקסל.

ניהול מידע עסקי מתבסס על המידע המתקבל מתהליכי הבקרה בממשק המשתמש והוא מאפשר הורדת עלויות והשאת רווחים מהמערכת התעשייתית. יחד עם זאת, דרך ממשק המשתמש ניתן גם להתאים ולשנות פרמטרים של תהליך הבקרה תוך מעקף מורשה של אמצעי הגנה וחומות אש, דבר המפחית את חוזק ההגנה והאבטחה בין ה- SCADA והרשתות העסקיות. השימוש באוגרי נתונים

למידע עסקי מצריך קונפיגורציה שתאפשר תקשורת עם ה- SCADA DMZ, וניתן וגם רצוי לעשות זאת ע"י שער חד כיווני (unidirectional gateway) כדי לשפר את האבטחה.

3. הפגיעות של רשתות תעשייתיות

יש הרבה דרכים לתקוף רשתות, אם כי בדרך כלל ישנם מספר שלבים בתהליך, כולל ריגול ולימוד מטרת התקיפה, סריקת הרשת, זיהוי מערכות הפעלה ומשתמשים (אנומרציה), וכמובן התקיפה עצמה. שלב הריגול מאפשר לתוקף למפות את הרשת ואת רמת האבטחה שלה, כולל שימוש בשירותי אינטרנט ומנועי חיפוש זמינים וכלים כגון Maltego[3], רשתות חברתיות, Social Engineer[4] Toolkit, וכדומה. סריקת רשת מתחילה בדרך כלל בניסיון לאתר התקנים ברשת, רשתות משנה, ושירותים שונים. גם כאן יש כלים שניתן להסתייע בהם, כגון Nmap[5], או Metasploit[6]. בשלב האנומרציה (Enumeration) מנסים לזהות משתמשים ומשאבים, וזאת ע"י ביצוע שאילתות שונות גם כאן תוך שימוש בכלים כגון Metasploit. התקפה יכולה להתבצע בכמה צורות תלוי במטרותיה, הפסקת שירות כלשהוא או שימוש מוסתר ברשת לאורך זמן. בשביל להפסיק או להפריע לשירות מסוים מספיק לדעת את כתובת ה- IP של השרת והפעלת התקפת מניעת שירות (DOS). לחלופין, יכול המתקיף לחדור לרשת ולהתקין בה קוד נוזקה (malware) כלשהו ולאחר מכן להשתלט למעשה עליה.

אפשר לסווג את התוקפים הפוטנציאליים לרשתות תעשייתיות לקבוצות הבאות:

- האקרים המחפשים יוקרה אישית
- מפעילי botnets וספאמרים
- פושעים המחפשים דרכים לשדוד כסף
- גורמים פנימיים כגון עובדים ממורמרים, שותפים עסקיים או טכנולוגיים
- גונבי זהויות ומבצעי phishing
- מחברי נוזקות ורוגלות
- שירותי ביון זרים
- טרוריסטים הרוצים להרוס תשתיות קריטיות
- מרגלים תעשייתיים המחפשים קניין רוחני

[3] http://www.paterva.com/web6/products/maltego.php
[4] https://www.trustedsec.com/downloads/social-engineer-toolkit/
[5] http://nmap.org/
[6] http://www.metasploit.com/

3.1 הערכת הפגיעות של רשתות תעשייתיות

נקודות החולשה של רשתות תעשייתיות ידועות ברובן. עשרות נקודות חולשה כאלה, לדוגמה, מתוארות במדריך לאבטחת מערכות בקרה תעשייתית (NIST SP 800-82)[7], החל בחולשות פרוצדוראליות (חוסר במודעות ובהנחיות ברורות), דרך חולשות בקונפיגורציה של הפלטפורמה (מערכות ללא טלאים, סיסמאות חלשות), חולשות של התוכנה (כגון שימוש בפרוטוקולים בעייתיים), חוסר בהגנה בפני נוזקות, חוסר בהצפנה ובבקרת גישה, וכן הלאה.

Table 3-12. Communication Vulnerabilities

Vulnerability	Description
Critical monitoring and control paths are not identified	Rogue and/or unknown connections into the ICS can leave a backdoor for attacks.
Standard, well-documented communication protocols are used in plain text	Adversaries that can monitor the ICS network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols such as telnet, File Transfer Protocol (FTP), and Network File System (NFS). The use of such protocols also makes it easier for adversaries to perform attacks against the ICS and manipulate ICS network activity.
Authentication of users, data or devices is substandard or nonexistent	Many ICS protocols have no authentication at any level. Without authentication, there is the potential to replay, modify, or spoof data or to spoof devices such as sensors and user identities.
Lack of integrity checking for communications	There are no integrity checks built into most industrial control protocols; adversaries could manipulate communications undetected. To ensure integrity, the ICS can use lower-layer protocols (e.g., IPsec) that offer data integrity protection.

לוח 3.1.1: נקודות חולשה הקשורות לתקשורת (לדוגמא)

גישה אלחוטית לרשתות תעשייתיות מוסיפה נדבך של בעיות פגיעות. מדובר במדיום משותף שאינו מאפשר אבטחה פיסית כך שהאקרים יכולים לנטר תנועה ברשת אלחוטית שאינה מיועדת אליהם ולבצע התקפות בנוסח man-in-the-middle. למרות פתרונות אבטחה כגון WiFi Protected Access (WPA) האקרים עדיין יכולים לפרוץ לרשת האלחוטית בגלל הגורם האנושי, הנטייה של משתמשים לבחור סיסמאות קצרות מדי שניתנות לחשיפה[8]. בנוסף לכך אותות אלחוטיים הנם רגישים למאמצי שיבוש וניתן, למשל, לבנות משבש GPS בעלות של כ- 30 דולר וכן גם לבצע התקפות Denial of Service ע"י הצפת נקודות גישה בבקשות אותנתיקציה. התקנים אלחוטיים רבים אינם כוללים הצפנה וניתן לצותת לתקשורת העוברת דרכם.

ניהול נקודות חולשה מחייב הערכה של הרשת ואיתור החולשות הקיימות, דבר המחייב בדיקה ידנית או שימוש בכלי אוטומאטי כגון Metasploit. כאשר מוצאים חולשה כזאת חייבים לתקן אותה ע"י יישום טלאי למערכת הקיימת, או התאמת הרשת והקונפיגורציה. אם המערכת היא קריטית ולא ניתן לתקן את החולשה יש צורך לבודד את החלק הרגיש. סריקת המערכת לצורך מציאת חולשות הנה

[7] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
[8] Francia et al, Cyberattacks on SCADA Systems, CISSE 2012
http://www.cisse.info/archives/category/29-papers?download=288:p02-2012

לעתים בעצמה תורמת לפגיעה ברשת בגלל סיבות שונות, כגון רגישות הפרוטוקולים, ולכן צריך לדעת איך לעשות זאת ללא הפרעה לפעילות השוטפת של הרשת.

הערכת נקודות חולשה ברשתות תעשייתיות הנה חלק מתקנים קיימים, כגון NERC CIP-007 (פרק 7) הכולל בין היתר דרישות לזיהוי שערים ושירותים פתוחים. ניתן להסתייע בכלים קיימים לצורך זה, לדוגמה CSET (Cyber Security Evaluation Tool) של מחלקת ביטחון הפנים של ארה"ב[9].

3.2 הקמת וניטור של מובלעות (enclaves) בטוחות

אסטרטגיה חזקה של הגנה לעומק מחייבת בידוד של קבוצות פונקציונאליות בצורה של מובלעות (enclaves) מאובטחות. לצורך זה יש לזהות את כל הקבוצות הפונקציונאליות והכוונה היא לכל המרכיבים המעורבים ישירות באותה פונקציה (התהליך קרוי גם סגמנטציה). כך למשל כל הנכסים המקושרים אחד למשנהו ברשת תקשורת (פיסית או לוגית) שייכים לקבוצה פונקציונאלית על בסיס תקשורת רשת. קבוצות פונקציונאליות יכולות להיות מבוססות על מעגלי בקרה, בקרת פיקוח, תהליכי בקרה, אחסון נתוני בקרה, גישה מרחוק וכדומה.

הגדרת קבוצות בהתבסס על שירותים, פרוטוקולים קריטיות וכדומה, היא דרך טובה להוציא התקנים מקבוצה. למרות זאת, התקנים רבים תומכים במספר פרוטוקולים, לדוגמה, ויכולים להשתייך למספר קבוצות ויש צורך להכליל אותם בקבוצות גדולות יותר. התהליך של הקמת מובלעות כולל זיהוי גבולות של כל מובלעת, התאמה של ארכיטקטורת הרשת למובלעת, תיעוד המובלעת לצרכי אכיפה ולצרכי קונפיגורציה.

אבטחת המובלעת נעשית על ידי הקמת אזור מאובטח אלקטרונית (Electronic Security Perimeter) סביב מובלעת מוגדרת המונע גישה ללא הרשאה למערכות במובלעת וכן גישה מהמערכות בתוך המובלעת החוצה. כדי להקים אזור כזה כל התקשורת פנימה אל המובלעת ומחוצה לה חייבת לעבור דרך חיבור רשת (או כמה חיבורי רשת) ידוע שניתן לבקרה ולניטור, וכן חייבים למקם התקן אבטחה (אחד או יותר) בכל אחד מן החיבורים הללו. כמינימום, התקן אבטחה כזה יכול להיות firewall, ובנוסף רצוי להתקין אבטחות נוספות כגון התקנים המזהים והמונעים חדירות (Intrusion Detection/Prevention) התקן לניהול איומים (Unified Threat Management), מנטרי יישומים, ועוד. רשימות התקני אבטחה מומלצים לפי רמת הקריטיות של המובלעות מצויות, לדוגמה, בתקן האבטחה NERC CIP המתואר בקצרה בפרק 6.

[9] http://ics-cert.us-cert.gov/Assessments

4. מיפוי תשתיות והתקנים המופעלים מרחוק

4.1 תשתיות והתקנים המופעלים מרחוק

תשתיות והתקנים רבים מנוטרים ומופעלים מרחוק והתחום קשור גם למה שקרוי תקשורת בין מכונות או M2M. השימוש במערכות SCADA החל כבר ב- 1960 כאשר נוצר צורך לניטור ובקרה יעילים של תשתיות בתחומים שונים, כגון תעשייה. בסוף שנות ה- 80 החלה מכירה של מערכות SCADA במחירים סבירים והשוק התפתח בקצב מהיר. סה"כ היקף השוק למערכות SCADA הוערך בכ- 6.6 מיליארד דולר ב- 2013, לעומת 2 מיליארד דולר ב- 2006[10]. המניעים העיקריים לצמיחה הם הצורך הגובר בתהליכים תעשייתיים אוטומאטיים, וכן הפריסה של פרויקטי smart grid בעולם. כיום סין תורמת קרוב למחצית מן ההכנסות ממכירת מערכות SCADA בעולם.

המושג M2M מתייחס לטכנולוגיות המאפשרות למערכות חוטיות ואלחוטיות לתקשר עם התקנים שונים, ובהגדרתו הרחבה כלל המושג גם את תחום ה- SCADA. ב- 1995 פיתחה חברת סימנס מודול מבוסס GSM המאפשר תקשורת בין התקנים (מכונות) ברשתות אלחוטיות. השוק של ה- M2M צומח כיום במהירות והוא מהווה למעשה חלק מתשתיות האינטרנט של הדברים (Internet of Things) המתואר בסעיף 4.3. היישומים של M2M הנם מרובים וכוללים סקטורים כגון בריאות, תשתיות (Utilities) ייצור תעשייתי, קמעונאות, חקלאות, שירותי חרום, אלקטרוניקה, תחבורה, ערים חכמות ובתים חכמים.

4.2 מהי תשתית קריטית?

בשנים האחרונות קיימת התייחסות הולכת וגוברת לפגיעותן של תשתיות חיוניות (או קריטיות) במדינות שונות. הפגיעות של התשתיות הללו נובעת, בין היתר, מן העובדה שהן מנוטרות ומופעלות מרחוק.

יש מספר הגדרות של מהי תשתית קריטית. במספר מדינות הקריטיות מתבססת על היעוד של התשתית, במדינות אחרות ההגדרה מתבססת על ההשלכות של פגיעה בתשתית על החברה. באיחוד האירופי ההגדרה של תשתית קריטית היא נכסים או מערכות שהנם חיוניים לקיומם של פעילויות חברתיות כגון בריאות, ביטחון, וכלכלה. בארה"ב ההגדרה מתייחסת למערכות או נכסים (פיסיים או וירטואליים) שהם חיוניים עד כדי כך שפגיעה בהם תהיה בעלת השלכות גדולות על ביטחון בכלל וביטחון כלכלי בפרט, וכן על בריאות הציבור[11].

ליאור טבנסקי מגדיר תשתית כחיונית (קריטית) אם שיבושה יוביל למשבר כלכלי-חברתי משמעותי עם השלכות פוליטיות אסטרטגיות וביטחוניות[12]. טבנסקי מציע שלושה ממדים להגדרת קריטיות של תשתית – המשקל הסמלי של התשתית (פגיעה באמצעי תקשורת יכולה לגרום לאובדן אמון של

[10] http://www.businesswire.com/news/home/20130722005859/en/Research-Markets-Global-SCADA-Revenues-Reached-6.6#.U3smwtJ_uvY

[11] Clemente, D., Cyber Security and Global Interdependence: What Is Critical? Chatham House 2013

[12] ליאור טבנסקי, "הגנה על תשתיות קריטיות פני איום קיברנטי", צבא ואסטרטגיה, כרך 3 גיליון 2, נובמבר 2011.

אזרחים בממשלה), התלות המיידית בתשתית (רשת האינטרנט למשל), וקשרי הגומלין בין תשתיות שונות אשר יכולים ליצור השפעות לא צפויות מעבר לפגיעה הנקודתית.

הגדרה זו תואמת למדי את ההגדרה של מחלקת ביטחון הפנים של ארה"ב:

"Critical infrastructure is the backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[13]

מעבר להגדרה הכללית של תשתית קריטית יש גם התייחסות וחלוקה לסקטורים קריטיים. המחלקה לביטחון פנים בארה"ב מפרטת 18 סקטורים קריטיים, כגון חקלאות ומזון, בנקאות ופיננסים, כימיקלים, תקשורת, ביטחון, וכן הלאה. הרשימה יחסית גדולה בהשוואה למדינות אחרות, ביפן רק 10 סקטורים ובבריטניה רק 9. בנוסף, יש גם התייחסות לתשתית מידע קריטית אם כי גם כאן ההגדרות שונות בין מדינה למדינה. האיחוד האירופאי מגדיר תשתית ICT קריטית כמערכות ICT שהן בעצמן קריטיות או שהן חיוניות לצורך תפעול תשתיות קריטיות אחרות. ארה"ב מגדירה תשתית מידע חיונית אם היא חיונית לתפעול תשתית קריטית אשר פגיעה בה תפגע גם בביטחון הלאומי או בביטחון הכלכלי או בבריאות הציבור.

דירקטיבת המדיניות הנשיאותית מספר 21 בארה"ב (PPD-21)[14] המתווה מדיניות לאומית עבור מחלקות וסוכנויות פדראליות לגבי זיהוי ומתן קדימויות לתשתיות קריטיות ומקורות חיוניים והגנתן מפני התקפות טרור. הדירקטיבה מתייחסת לתשתיות ולסקטורים הבאים – כימיה, מתקנים מסחריים (אצטדיונים, מוזיאונים, בתי מלון, פארקים, קניונים, וכדומה), תקשורת, מתקני הייצור הקריטיים (ייצור מתכת, ייצור מכונות, ייצור ציוד אלקטרוני, ייצור ציוד תקשורת), סכרים, תעשיות הביטחון, שירותי חירום (משטרה, כבאים, רפואה בחירום וכדומה), ייצור אנרגיה (חשמל, נפט, גז), שירותים פיננסיים, מזון וחקלאות, מתקנים ממשלתיים (משרדים, שגרירויות, בתי משפט, מעבדות לאומיות, וכדומה), שירותי רפואה, טכנולוגיית מידע (ייצור חומרה, תוכנה ומערכות מידע), כורים גרעיניים, תחבורה ומים. האחריות לאבטחת כל אחד מן הסקטורים הללו מוטלת על משרדי מספר ממשלה, ברוב המקרים זוהי המחלקה לביטחון פנים. לכ אחד מן הסקטורים הללו יש תכנית ספציפית להגנה על תשתיות בפני התקפות סייבר.

[13] http://www.dhs.gov/what-critical-infrastructure

[14] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

בקנדה תשתיות קריטיות הוגדרו בדו"ח משנת 2010 אשר זיהה 10 מגזרים של תשתיות קריטיות והעניק את האחריות להגנתן על מחלקות וסוכנויות פדראליות מתאימות. המגזרים שזוהו הם[15]:

- Energy and Utilities: Natural Resources Canada
- Information and Communications Technology: Industry Canada
- Finance: Finance Canada
- Food: Agriculture and Agri-Food Canada
- Health: Public Health Agency of Canada
- Manufacturing: Industry Canada, Department of National Defence
- Safety: Public Safety Canada
- Transportation: Transport Canada
- Water: Environment Canada

תשתיות בסיסיות, כגון מים, גז, נפט, חשמל ותקשורת, הן תשתיות קריטיות הנסמכות באופן נרחב על רשתות תעשייתיות ומערכות בקרה אוטומאטיות. מאחר והפרעה לתפעול התקין של תשתיות כאלה משפיעה על החברה והכלכלה, הן מזוהות כקריטיות ב- HSPD-7, מאחר והן מערכות אוטומאטיות הכוללות תהליכי בקרה מבוזרים. תשתית החשמל בדרך כלל מצריכה אבטחה יותר נוקשות ובארה"ב וקנדה יש רגולציה ספציפית ותקנים של אמינות וביטחון סייבר[16].

מתקנים גרעיניים מהווים אתגר מיוחד בגלל הסכנות הטמונות בתדלוק ובתפעול שלהם ולכן הם מהווים מטרה מועדפת למתקפות סייבר. לכן קיימת רגולציה מחמירה בארה"ב על ידי נציבות הרגולציה הגרעינית (NRC).

מערכות ייצור והובלת חשמל מהווים תשתית קריטית והן כפופות לרגולציה מחמירה על ידי NERC (North American Electric Reliability Corporation), במיוחד דרך תקני האמינות המפותחים תחת ההשגחה של מחלקת האנרגיה בארה"ב האחראית לביטחון בייצור, זיקוק, הפצה ואחסון של נפט וגז. צריך להבחין בין ייצור חשמל להובלת חשמל, שהן שתי רשתות שונות המצריכות אבטחה שונה אם כי יש ביניהן חיבוריות ולדברים אלה מתייחס תקן היעילות שנוצר על ידי NERC (הקרוי הגנה על תשתיות קריטיות).

במתקנים לייצור והפצה של חומרים כימיים יש גם צורך להגן על זכויות יוצרים מפני שלמוצרים יש גם ערך לא מוחשי.

[15] Gendron, A., and Rudner, M., Assessing Cyber Threats To Canadian Infrastructure, CSIS/SCRS 2012

[16] Eric Knapp, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA' and other Industrial Control Systems, Syngress Publishing 2011

בתחילת שנת 2013 נערך סקר[17] של תשתיות קריטיות על ידי Cloud Security Alliance כתגובה ל-RFI של הממשל האמריקני אשר ביקש חוות דעת בנושא של שיפור ההגנה על תשתיות קריטיות. הנשאלים נתבקשו לדרג את מידת הקריטיות של תשתיות שונות והתוצאות מתוארות בלוח הבא.

Sector	CI Rating Average (4.0 most critical)
Water supply	3.87
Information and communications	3.80
Electric power	3.67
Emergency law enforcement services	3.47
Emergency fire service	3.47
Banking and finance	3.40
Oil and gas production and storage	3.33
Public health services	3.27
Highways (including trucking)	3.20
Pipelines	3.20
Mass transit	2.87
Rail	2.87
Aviation	2.80
Waterborne commerce	2.67
Continuity of government services	2.67

4.3 מבט קדימה על תשתיות שיהפכו לקריטיות בעתיד

תעשיית הרכב העולמית תעבור בעתיד למערכות ניהוג אוטונומיות והמשמעות היא קישור של כלי הרכב בינם לבין עמם וכן למוקדי תעבורה. המשמעות היא שניתן יהיה לשלוט בכלי הרכב ממרחק על המשמעויות החיוביות והשליליות הכרוכות בכך. בכנס Defcon האחרון הראו שני מומחי אבטחה איך הם הצליחו לפרוץ את מאפייני הנהיגה העצמית של שתי מכוניות פופולאריות[18]. מכוניות ללא נהג הם בעצם רובוטים מתוחכמים שהנם רגישים לפריצות כמו רובוטים פחות מתוחכמים. רגישויות אלה יכולות להיות קשורות לפריצה לרשתות החיישנים (כגון GPS, LIDAR, מצלמות, רדאר מילימטרי ועוד) שמהוות בסיס לניהוג אוטונומי של מכוניות. התקפות על רשתות חיישנים יכולות לגרום לכך שהחיישנים יפסיקו לפעול או שיקבלו נתונים שגויים.

אחת מן המגמות הבולטות אשר ישפיעו על חיינו בשנים הקרובות היא ההתפתחות של האינטרנט של הדברים (Internet of Things - IoT). זו תהיה רשת גלובלית דינמית המתפתחת כל הזמן, משתנה, מתאימה את עצמה, משנה את הסקאלה שלה וכן את הקונפיגורציה שלה. בשינוי קונפיגורציה הכוונה היא ליכולות ארגון עצמי, ריפוי עצמי, ניהול עצמי, אוטונומיה, מודעות להקשר

[17] Executive Order – Critical Infrastructure Survey Results, Cloud Security Analysis
[18] http://news.cnet.com/8301-1009_3-57596847-83/car-hacking-code-released-at-defcon/

ומודעות לרשת. "דברים" ברשת ניתנים לזיהוי ובעלי מאפיינים פיסיקאליים המאפשרים להם לחוש, להפעיל, להגיב, להתממשק ולתקשר. מספר היישומים האפשריים הוא גדול מאד. פרויקט אירופאי בשם IoT-I מיפה בשנת 2010 65 יישומי IoT ב- 14 תחומים, כולל תחבורה, הבית החכם, עיר חכמה, סגנון חיים, קמעונאות, ייצור חכם, שרשרת הספקה, חירום, בריאות, וכן הלאה[19]. מושג קרוב לאינטרנט של הדברים הוא מערכות סייבר-פיסיקליות (Cyber-Physical Systems) המהוות אינטגרציה של מחשוב, רישות, ותהליכים פיסיים[20]. עצמים המחוברים לרשת האינטרנט של הדברים יכולים להיות חשופים להתקפות סייבר במידה ואינם מוגנים, כגון לפגיעות נוזקה שתגייס אותם לרשת בוטנט, או להיכנס למכשירים חכמים בבתים ולסגור אורות, לפוצץ מגברים במערכות אודיו, לפתוח דלתות ושערים, וכן הלאה.

5. ראיונות עם מומחים

במשך המחקר נערכו מספר ראיונות עם מומחים מן התעשייה והאקדמיה בישראל. מטרת הראיונות הייתה לקבל מידע ראשוני על הבעיות הכרוכות בניטור והפעלה של תשתיות והתקנים מרחוק בישראל, כולל התייחסות לתשתיות קריטיות. להלן סיכום תמציתי של דבריהם.

תשתיות קריטיות:

מספר התשתיות הקריטיות הוא גדול יחסית והוא כולל שירותים, תשתיות ואנשים. הקריטריונים לקריטיות כוללים פגיעה בחיי אדם, פגיעה כלכלית, וכן פגיעה מהותית בסדר הציבורי. תשתיות המופעלות מרחוק הנן רגישות לתקיפה דרך הבקרה עליהן או באמצעות הרשת או באמצעות החדרה פיסית אל ההתקן עצמו. הבקרים הללו נמצאים במקומות לא מאוישים והם מעבירים נתונים למרכז הבקרה. הפרוטוקולים הנפוצים ברשתות הבקרה הם Mudbus ו- DNP3 הוותיקים אשר ידועים ברגישותם לפריצה ומשלוח של פקודות עוינות. עם הזמן חלו שיפורים שונים בפרוטוקולים ופותחו תקנים חדשים עם אפשרויות הגנה משופרות כנגד מתקפות סייבר.

ישנם הרבה מערכות שלא היו מחוברות לרשת בעבר ואולי אף אינן נחשבות כקריטיות כיום אבל הן תהיינה מחוברות בעתיד. הסביבה המורכבת בחיבוריות שלה לרשת והתלות של מערכות זו בזו יוצרים יחד תשתית פורייה למתקפות שונות. לכן יהיה צורך להוסיף יותר ויותר מערכות למערך הגנת הסייבר.

מיפוי הרשת הוא האתגר הראשון בתהליך האבטחה כנגד איומי סייבר. יש צורך לגלות ולאפיין את כל הקישורים החוצה כי הם בעצם גם דלת כניסה. ספקים כמו סימנס מתעקשים להתקשר לרשת מבחוץ ואז צריך לאפיין את מהות הקישור. יש אפשרות לתקשורת חד-כיוונית או לתקשורת מאובטחת עם מפתחות.

[19] IoT-I, Internet of Things Initiative, FP7 EU project, FP7-ICT-2009-5-257565
[20] http://cyberphysicalsystems.org/

בשנים הקרובות היכולות שקיימות כיום אצל מדינות יזלגו לארגוני פשע, ולכן אנו נראה אירועים שבהם ארגוני פשע יסחטו את התשתיות האסטרטגיות על ידי תקיפות שונות.

תפקיד המדינה כרגולטור:

המדינה מנחה כרגולטור אם היא מגדירה משהו כקריטי לפי קריטריונים מוגדרים. הבקרה של הרגולטור הינה בקרה מפצה המתקיימת בנוסף לבקרה של הגוף המבוקר על עצמו באופן שוטף. תחת הנחיה יכולות להיכנס תשתיות של ממש או שירות או חיי אדם שהינם בסיכון,ולאו דווקא כמו התפיסה שמדובר רק בתשתיות כמו מפעלים.

מעבר לטיפול בתשתיות הקריטיות הציבוריות קיימת גם התייחסות לתשתיות פרטיות. אל מול מתקני התשתית הפרטיים בישראל פועל משרד התשתיות הלאומיות האנרגיה והמים בכל הקשור להגנה ואבטחת מערכות המחשב החיוניות במתקנים אלו,זאת במסגרת אחריותו הרגולטורית. בעזרת נוהל שנכתב במשרד, מתקיים תהליך הכוונה ליווי והנחיה של מתקני תשתית פרטיים (לדוגמא במגזר הגז החשמל והמים) להגנה על מערכות המחשב החיוניות של מתקנים אלו. תהליך הכוונה וליווי זה משרת את אינטרס שני הצדדים מחד הבטחת הרציפות התפקודית של המתקן ואידך את רציפות התפקודית של המגזר המטופל.

נקודות אפשריות לשיפור:

אפשר לבצע שיפור תהליכים בזמן זיכוי תוכנה, דהיינו יצירת תהליך שבודק מה יש בתוכנה שסופקה בפועל לעומת מה שאמור להיות בה וזאת כדי לזהות רוגלות מובנות. יש לבנות סדנה שתעורר טריגרים שיאפשרו איתור קוד עוין, וכן גירויים נוספים שידמו סביבה אמיתית וכך יעוררו את הקוד העוין.

המדינה, הצבא והעיריות השונות צריכים להיערך למצבי חירום. יש להתמודד עם אירועי סייבר באופן קלאסי ממוחשב. יש לגבות את המערך עם פתרונות ישנים לשעת חירום. מים, חשמל והלאה הינם דברים קריטיים ולכן צריך לתת לדאוג לחלופת אספקה בחירום,ולהבין שהמחשב הינו הגורם שנותן למים את הפקודות לזרום. יש צורך באבטחה של מערכות מזון ומערכות לניהול מלאי.

המדינה צריכה לממן תקנים המיועדים להתמודדות עם אירועי סייבר בשעת חירום. יש צורך בעתיד לתקנן תקנות בטיחות ונהלים שמסתכלים על בניית ה- SCADA בעין משפטית.

6. מדיניות אבטחת תשתיות כולל תקנים בינ"ל

6.1 תקנים[21]

סקטור החשמל, תקני האמינות **NERC CIP**: אלה תקנים צפון אמריקניים להגנה על אמינות תשתיות חשמל קריטיות הבנויים מתשע בקרות לניהול קונפיגורציה נפרדות: דיווח על חבלות, זיהוי נכסי סייבר קריטיים, בקרות של ניהול אבטחה, עובדים והדרכה, מרחבי אבטחה אלקטרונית, אבטחה פיסית של נכסי סייבר קריטיים, ניהול אבטחת מערכות, דיווח על אירועים ותכנון תגובה, וכן תוכניות להתאוששות של נכסי סייבר קריטיים.

סקטור הכימיקלים – **CFATS**: תקנים להגנה של מפעלים כימיים בפני טרור המציינים איזה בקרות נדרשות, כגון (RPBS 8 או Cyber Metric 8) מדיניות אבטחה, בקרת גישה, אבטחת עובדים, מודעות והדרכה, ניטור ותגובה לאירועים, התאוששות מאסון והמשכיות עסקית, פיתוח ורכש של מערכות, ניהול קונפיגורציה, וכן ביקורת. כך לדוגמה, קטע Cyber Metric 8.2.1 דורש שגבולות המערכת יזוהו ויאובטחו באמצעות בקרות היקפיות, דבר התומך במודל האבטחה של מובלעות (enclaves).

תקן ISO **ISO/IEC 27002:2005**: תקן בינ"ל של ארגון התקנים הבינ"ל (ISO), IEC (International Electrotechnical Commission), ושל מוסד התקינה האמריקני (ANSI), הממפה תקני אבטחה במדינות רבות. התקן מתבסס על מודל אבטחת המידע של הסי אי איי עם הקדימויות של חשאיות, שלמות וזמינות. התקן מתמקד בהערכת הסיכון ובמדיניות האבטחה בנוסף לבקרה של האבטחה הטכנית. הבקרות הטכניות כוללות ניהול נכסים, ניהול קונפיגורציות, בקרת אבטחה של תקשורת הרשת, וכן בקרת אבטחת הגישה והגנה בפני נוזקה. הדגש הוא במיוחד על קבוצה של בקרות העוסקות בניהול אירועי אבטחה, כגון זיהוי אנומליות.

תקן אבטחת סייבר **NRC Regulation 5.71**: רגולציה זו מספקת המלצות אבטחה שהן בקנה אחד עם סעיף 10 ברגולציה הפדראלית 73.54, הכוללת דיון מעמיק על הדרישות של אבטחת סייבר, כולל תכנון והקמה של תכנית כזו. התכנית כוללת שימוש ברשת של 5 אזורים נבדלים עם תקשורת חד-כיוונית בין אזור 0 ל- 1 (המובלעות הקריטיות ביותר מבין 5 האזורים). שערים של תקשורת חד-כיוונית, כגון דיודות של נתונים, מאפשרים תקשורת החוצה ומונעים תקשורת חוזרת ובכך מאפשרים תקשורת מאובטחת.

המדריך לאבטחת מערכות בקרה תעשייתיות של NIST (**NIST SP 800-82**): המדריך כולל המלצות לאבטחה, ניהול, תפעול, ובקרה טכנית לצורך שיפור רמת האבטחה של מערכות בקרה. המדריך הוא עדיין ברמת טיוטה והוא מייצג המלצות ולא רגולציה. למרות זאת, הבקרות המוצגות במדריך הנן מקיפות ומשתלבות היטב בהמלצות אחרות של NIST.

[21] מתבסס על Knapp פרק 10

התכנית לשיפור אבטחת סייבר של תשתיות קריטיות (**Framework for Improving Critical Infrastructure Cybersecurity**) פורסמה ע"י NIST בתחילת 2014[22]. התכנית באה בעקבות הנחייה נשיאותית (executive order) מ- 2013 שבמסגרתה הוחלט להכין תקנים על בסיס וולונטרי כדי לסייע לארגונים שונים לנהל נכונה את סיכוני הסייבר שלהם. התכנית מתחלקת לתכניות משנה כולל ליבת התכנית, פרופיל התכנית ויישום התכנית. התכנית כוללת גם מתודולוגיה לשמירה על הפרטיות של המשתמשים. ליבת התכנית כוללת רשימת פעילויות אבטחה בתהליך כולל זיהוי איומים וסיכונים, הגנה בפני איומים, איתור וזיהוי של איומים כאשר הם מופעלים, הכנת תגובה וטיפול באיומים המתרחשים, וכן התאוששות ושרידות של התשתית לאחר שהאיומים מתרחשים.

6.2 מדיניות אבטחת תשתיות במדינות שונות

ארגון ה- OECD סקר לא מכבר את מדיניות ואסטרטגיות הסייבר סקיוריטי של 10 מדינות OECD שונות[23]. מדיניות להגנת מרחבי הסייבר ותשתיות קריטיות הקשורות אליהן נמצאת כבר בעדיפות לאומית גבוהה במדינות השונות. הדגש במדיניות הגנה מתרחב מהגנה על פרטים וארגונים להגנה על החברה כולה. האחריות על הגנת סייבר היא על הממשלה אם כי מדובר בדרך כלל על תיאום של מספר ישויות ממשלתיות בגלל המורכבות והביזור הגדול של נושא הסייבר על פני תחומים רבים. יש הכרה בכך שתשתיות הסייבר רובן בבעלות פרטית ויש להן השלכות גלובליות, ולכן יש צורך בשיתוף פעולה עם הסקטור הפרטי וכן שיתוף פעולה בינ"ל. כל האסטרטגיות שמות דגש חזק על הצורך של המדיניות לכבד זכויות בסיסיות כגון פרטיות, חופש ביטוי, וזרימה חופשית של מידע. בנוסף לכך, יש הכרה בכך שיש צורך במעורבות כוללת גם של גורמים ביטחוניים וצבאיים, יש גם הכרה בחשיבות של אספקטים הכלכליים של מדיניות הסייבר, וכן הכרה בצורך של ניהול דיאלוג עם גורמים לא ממשלתיים.

תכניות הפעילות של אסטרטגיות הגנת הסייבר כוללות בדרך כלל את המרכיבים הבאים:

- יוזמות לאבטחת הממשלה
- הגנה על תשתיות מידע קריטיות
- מלחמה כנגד פשיעת סייבר
- העלאת המודעות לנושא
- חינוך והכשרת כוח אדם להגנת סייבר
- גיבוש צוותים לצורך מתן תגובה על אירועי סייבר

חלק מן האסטרטגיות של המדינות שנסקרו כוללות גם נושאים חדשים כגון:

- פיתוח יכולות מודעות לסיכונים (situational awareness) וניטור בזמן אמת, בעיקר עבור תשתיות ממשלתיות

[22] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[23] OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy

- מדיניות תמיכה בתעשיות אבטחת סייבר
- אפיון והגדרה של סקטורים וארגונים כתשתיות מידע קריטיות
- שותפויות עם ספקי אינטרנט כנגד איומי botnet
- זיהוי כוחות מניעים כלכליים ותמריצים כגון הודעות על פגיעה בפרטיות או תיוג מוצרים ושירותים
- תרגולות אבטחת סייבר כולל שיתוף מדינות זרות
- פיתוח של מסגרות לזיהוי דיגיטאלי
- מדיניות ספציפית להגנה על ילדים באינטרנט

ארגון אירופאי הקרוי ENISA (European Network and Information Security Agency) ערך לא מכבר מדריך פרקטי לפיתוח וביצוע של אסטרטגיות הגנת סייבר לאומיות[24]. המדריך מתאר בפירוט 20 פעולות קונקרטיות הנדרשות כדי לגבש אסטרטגיה כזו, כולל חזון יעדים וקדימויות, הערכת סיכונים לאומית, ניתוח מדיניות קיימת, מבנה ניהולי, זיהוי בעלי עניין, שיתוף במידע, וכן הלאה.

6.3 מדיניות אבטחת תשתיות בישראל

מדיניות אבטחת התשתיות הקרויה גם הגנה קיברנטית מתוארת במסמך של מרכז המחקר והמידע של הכנסת שפורסם לאחרונה[25]. כבר ב- 2002 החליטה הממשלה לקבוע את האחריות להגנה על מערכות ממוחשבות בישראל, כולל הקמת ועדת היגוי שתבחן אלה גופים יוגדרו כחיוניים ולכן זקוקים להגנה קיברנטית אשר תסופק באמצעות יחידה ייעודית של השב"כ והיא הרשות לאבטחת מידע (רא"מ). גופים חיוניים כגון משרד הביטחון, המוסד וצה"ל מנהלים את האבטחה הקיברנטית בעצמם, ולא דרך רא"מ.

הבסיס החוקי לאבטחה הקיברנטית בישראל מבוססת על החוק להסדרת הביטחון בגופים ציבוריים (התשנ"ח-1998) הקובע סמכות ואחריות לאבטחה פיסית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות של גופים ציבוריים[26]. החוק קובע חובה למנות ממונה ביטחון בגופים הציבוריים אשר יהיה כפוף לקצין מוסמך אשר יספק הנחיות מקצועיות. לחוק יש ארבע תוספות, כאשר בתוספת הראשונה רשימת גופים המונחים ע"י השב"כ הן באבטחה פיסית והן באבטחת מידע (משרד ראש הממשלה, משרד הביטחון, מפעלי מערכת הביטחון, לשכת נשיא המדינה ומשרד החוץ). בתוספת השנייה נמצאים גופים שמונחים ע"י השב"כ בנושאי אבטחת מידע וע"י המשטרה בנושאי אבטחה פיסית (משרדי ממשלה אחרים, הסוכנות, רשות השידור, חברת חשמל, בזק, החברות הסלולאריות, ועוד). בתוספת השלישית מצויים גופים המונחים רק בנושאי אבטחה פיסית ע"י המשטרה (קק"ל, האוניברסיטאות, וכן הלאה). בתוספת הרביעית נמצאים גופים המונחים בידי השב"כ בנושאי אבטחת

[24] ENISA, National Cyber Security Strategies: Practical Guide on Development and Execution, December 2012

[25] רועי גולדשמיט, המרחב הקיברנטי וההגנה על תשתיות חיוניות, מרכז המחקר והמידע, הכנסת 12 במאי 2013

[26] שם, עמוד 7

מערכות מחשוב חיוניות (בזק, בנק ישראל, בתי הזיקוק, חברת חשמל, מקורות, רכבת ישראל, רשות שדות התעופה, חברות התקשורת הסלולארית, ועוד).

מיזם לאומי להתמודדות עם האיום הקיברנטי (המטה הקיברנטי הלאומי) הוקם ב- 2010 על ידי הממשלה ותכנית העבודה שלו הוכנה ע"י פרופסור יצחק בן ישראל. המטה עוסק בהסדרה ותכלול הפעילות הכלל ממשלתית הנוגעת למרחב הקיברנטי בראייה אזרחית וביטחונית ולמעשה פועל לגיבוש מדיניות הגנה כוללת למרחב הקיברנטי. תפקידי המטה הנם לייעץ לממשלה בנושא הקיברנטי, לרכז את עבודת המטה הממשלתית בתחום, להמליץ לראש הממשלה על מדיניות קיברנטית לאומית, לפרסם הנחיות מדיניות, לקדם תיאום ושיתוף פעולה, וכן לקדם חקיקה ותקינה בתחום הקיברנטי[27]. ההחלטה על הקמת המטה התקבלה באוגוסט 2011[28], והמטה עצמו החל לפעול בתחילת שנת 2012.

[27] http://www.pmo.gov.il/BRANCHESANDUNITS/CYBER/Pages/default.aspx

[28] החלטת ממשלה מספר 3611, "קידום היכולת הלאומית במרחב הקיברנטי", 7 באוגוסט 2011