|  |  |  |
| --- | --- | --- |
| **clalit** | cybermed2 | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Logo_CSRC.PNG |
|  | Logo_Malware_Lab |

**מערכת הגנה אקטיבית למוניטורים רפואיים**

מסמך אפיון

סטודנטית: רותם לזר.

הנחיה רפואית: ד"ר יצחק לזר.

הנחיה אקדמית: ד"ר ניר ניסים.

המחקר מבוצע במסגרת פרוייקט Cyber-Med במעבדת הפוגענים (Malware Lab)

המרכז לחקר הגנת הסייבר של אוניברסיטת בן גוריון בנגב.

גרסה 1.0

12/12/16



**1. הקדמה**

בשלל בתי חולים בארץ ובעולם, משתמשים במוניטורים. מוניטורים אלה מציגים מידע על החולה שאליו הוא מחובר, לדוגמה דופק, לחץ דם, חום גוף ועוד. למידע המוצג על המוניטור חשיבות קלינית רבה, מאחר ועל פיו נקבעות התרופות הניתנות ואופי הטיפול בחולה. בנוסף, מוניטור החולה, ככלי אשר מרכז את רישום הסימנים החיוניים של החולה, מחובר למערכת "תיק חולה אלקטרוני" אשר מתעד את כל המידע אשר נאסף מהחולה בכל דקה, וקשורה למאגרי המידע של בית החולים. מאגרים אלה כוללים, בין היתר, את מערך המעבדות, בדיקות ההדמיה והרנטגן, ארכיון המתעד אשפוזים קודמים ומכתבי שחרור ועוד. לכל המוניטורים יש כרטיס רשת אלחוטית וכניסות לחומרה ניידת (Wi-Fi), אשר נחסמו בעקבות העובדה שהמוניטורים אינם מוגנים והינם חשופים למתקפות. חדירה אל מוניטורים אלו יכולה להוביל לשינוי המידע המוצג עליהם וכתוצאה לשבש את הטיפול שהרופא יעניק לפציינט, כמו גם לחדור לתוך רשת בית החולים. כאמור, רשת זו מכילה מידע רגיש וסודי בנוגע לכל אדם שטופל בבית החולים, מידע שבית החולים וכן מערכת הבריאות בכלל מחויבים לשמור בסודיות.   
אנו משערים כי המוניטורים, ככל כלי אלקטרוני דיגיטלי, חשופים לפריצות זדוניות היכולות לשנות את המידע המוצג על ידיהם או לשבש ולהפסיק את פעילותם (מתקפת DOS), והעובדה כי המוניטורים מחובר ים לרשת, יכולה להוות נקודת חדירה לרשת בית החולים.

1.1 מטרה

*מטרת הפרויקט היא לחקור את פגיעותם של מוניטורים בפני חדירה זדונית למידע המוצג והנאסף על ידם ו/או להשתמש במוניטור כנקודת חדירה לרשת בית החולים.*

*ישנן מספר דרכים שבהן ניתן לפגוע בתפקוד המוניטור או המערכת שמחוברת אליה:*

*דרכי פגיעה במוניטורים:*

|  |  |
| --- | --- |
| *פגיעה* | *תוצאה* |
| *מניעת העברת מידע בין החולה לבין המוניטור* | *המערכת אינה מציגה מידע חיוני אודות החולה, ובעקבות כך אינה יכולה להתריע במקרה של סכנה* |
| *השתקת האזעקה* | *המערכת אינה מציגה מידע חיוני אודות החולה, ובעקבות כך אינה יכולה להתריע במקרה של סכנה* |
| *ערבול התצוגה* | *מידע חיוני אודות החולה הוא שקרי/קשה לקריאה ופענוח* |
| *גרימה לאיבוד פקטות של מידע בתקשורת ברשת* | *פגיעה במידע המועבר אודות החולה* |
| *הצגת מידע שקרי על המוניטור* | *חברי צוות הטיפול מקבלים מידע שקרי אודות החולה* |
| *אי-הודעת מקרה רפואי* | *פוגע בטיפול החולה* |
| *הודעה אל מקרה רפואי שקרי* | *חברי צוות המטפלים מקבלים החלטות שאינן מתאימות לחולה* |

*דרכי פגיעה במערכת המחשוב אשר אוספת את המידע מהמוניטור (EMR):*

|  |  |
| --- | --- |
| *פגיעה* | *תוצאה* |
| *מניעת העברת מידע בין החולה לבין המוניטור* | *המערכת לא מספקת מידע אודות החולה, יש לבצע שוב את הבדיקה/מדידה...* |
| *מחיקה או שינוי מידע המוזן במערכת* | *המערכת לא מספקת מידע אודות החולה, יש לבצע שוב את הבדיקה/מדידה...* |
| *ערבול התצוגה* | *מידע חיוני אודות החולה הוא שקרי/קשה לקריאה ופענוח* |
| *גרימה לאיבוד פקטות של מידע בתקשורת ברשת* | *פגיעה במידע המועבר אודות החולה* |
| *הצגת מידע שקרי במערכת* | *חברי צוות הטיפול מקבלים מידע שקרי אודות החולה* |
| *הודעה על מקרה רפואי שקרי* | *חברי צוות המטפלים מקבלים החלטות שאינן מתאימות לחולה* |

*לאחר שנאפיין את נקודות הפגיעות והתורפה של המוניטור, נבנה כלי אשר יוכל להגן על המוניטור והרשת שאליה הוא מחובר. כלי זה יגן על המוניטור ולא יאפשר חדירה דרך שלל כניסות אפשריות (אינטרנט אלחוטי וחוטי, חומרה ניידת ועוד).*

1.2 המוצר

*חלק זה צריך להכיל את הדברים הבאים:*

* **שם המוצר אותו מפתחים (ובאמצעותו נתייחס למוצר בהמשך המסמך)**

*שם המוצר:* ***מינוטאור****- מערכת הגנה אקטיבית למוניטורים רפואיים*

* **הסבר כללי של מה המוצר עושה (ואם צריך- מה הוא לא עושה)** *1. אפיון פגיעות המוניטור  
  2. בניית הגנה לחדירה*
* **תיאור של מטרות המוצר ויתרונותיו העיקריים. נסו להיות מדויקים וספציפיים כמה שניתן.**

*מטרות המוצר :*

1. *התרעה והתראה למנהל המידע על ניסיון חדירה למערכת או שינוי מידע הנקלט.*
2. *חסימת ההתקפה ומניעת חדירה לרשת.*
3. *דיגול (Flagging) המידע ששונה במערכת.*
4. *בידוד התוכנה התוקפת לשם חקירה.*

1.3 הגדרות

**בחלק זה יש לציין את כל ההגדרות, המושגים וראשי התיבות בהם תשתמשו בהמשך המסמך.**

* *מוניטור- כלי אלקטרוני אשר קולט מידע מחיישנים על גוף הנבדק, מציג אותו באופן ויזואלי על פני מסך ושולח את המידע הנאסף אל מערכת EM*
* *מערכת EMR (Electroncial Medical Record) – מערכת ממוחשבת אשר מחליפה את גיליון החולה מנייר. מערכת זו אוספת מידע עדכני בכל דקה משלל מכשירי הניתור והטיפול האלקטרוניים אשר תומכים בחולה. היא מחוברת לרשת המידע של בית החולים. (נקראת גם EHR – Electronic Health Records)*
* *DOS Attack- (Denial Of Service) משפחת מתקפות אשר מונעות או פוגעות בשימוש ברשתות, מערכות או אפליקציות בכך שנוצר עומס חריג על חלק ממשאבי המערכת.  
  1. Buffer over DOS- מתקפה אשר מציפה שרת של רשת בכמות גדולה של מידע.*

*2. Smurf DOS- מתקפה אשר גורמת למחשבים שונים ברשת להיענות לבקשות מזויפות ובכך ליצור תעבורה רבה (דבר אשר מאט מאוד את התקשורת ברשת)*

* *~פה נכניס שמות של צורות התקפה אשר עלולות לפגוע במוניטור, ודרכו ומערכת הEHR שאליה הוא מחובר. בהמשך המחקר, יתווספו למסמך זה מושגים נוספים~*

**1.4** תקציר

**הסבר מה מופיע בהמשך המסמך ופירוט כיצד זה מסודר לאורך המסמך**

במסמך זה אפרט את מהלך העבודה בפרויקט.   
בשלב הראשון, כאמור, אאפיין את המוניטור עליו אעבוד מבחינת תכונות קלט-פלט, רשת אלחוטית, רשת קווית וכניסות נוספות אשר מאפשרות חדירה את המערכת. אלמד את הפרוטוקולים השונים עמם עובד המוניטור.   
בשלב השני, אתמקד בהבנת הדרכים בהן ניתן לפגוע במידע המועבר מהחולה אל המוניטור ומשם אל מערכת הEMR.   
בשלב השלישי, אבחן את התכנות הזדונית אשר יכולות לפגוע במערכת שאפיינתי בשלב הקודם.   
בשלב הרביעי אבנה תוכנות הגנה למניעת החדירה, התראה והתרעה על ניסיון החדירה, בידוד ומניעת נזק היעשה על ידי התוכנה הזדונית.

1. הקדמה:
   1. הקדמה
   2. מטרה
   3. המוצר
   4. הגדרות
   5. תקציר
2. תיאור כללי:

2.1 פונקציונליות

2.2 קהל היעד

2.3 אילוצים עיקריים

2.4 הנחות ותלויות

2.5 סיקור השוק כיום

1. דרישות מפורטות:

3.1 דרישות פונקציונליות

3.2 דרישות של ממשקים חיצוניים

3.3 דרישות לא פונקציונלית

3.4 דרישות בסיס נתונים

3.5 דרישות נוספות

1. בבליוגרפיה
2. תיאור כללי

החלק הזה מתאר את הגורמים העיקריים המשפיעים על המוצר ועל דרישותיו. חלק הזה לא מפרט דרישות ספציפיות אלא רק עוזר להבין את הדרישות.

2.1 פונקציונליות

**חלק זה יכיל סיכום של הפונקציות העיקריות במערכת (לא פונקציות של שפת תכנות, אלא באופן מילולי - מה הדברים שהמערכת עושה)**

1. *פונקציה המזהה התקפות זדוניות המכוונות לפגיעה במוניטור אשר מגיעות מרשת אלחוטית שאליו הוא מחובר.*
2. *פונקציה המזהה ומתריעה למנהל המידע על ניסיון חדירה למערכת או שינוי מידע הנקלט.*
3. *פונקציה החוסמת את ההתקפה ומונעת חדירה לרשת.*
4. *פונקציה העושה דיגול (Flagging) למידע ששונה במערכת.*
5. *פונקציה המבודדת את התוכנה התוקפת לשם חקירה.*

2.2 קהל היעד

**תיאור כללי של קהל היעד של המערכת - מה תפקידם, ניסיונם, יכולתם ללמוד את ממשק המערכת וכל דבר אחר שישפיע על דרישות המערכת. יתכן יותר מפרופיל אחד של משתמש במערכת, ולכן יש לפרט את כל הסוגים וההשלכות/משמעויות שלהם מבחינת אופי ורקע טכנולוגי או פונקציונלי. ("מי הולך להשתמש במערכת?")**

*קהל היעד של הכלי אותו אפתח הם עובדי מערכת הבריאות בעולם וכן חברות המייצרות את המוניטורים הללו. דוגמה לגוף אשר יכול להשתמש בכלי שאותו אפתח, היא ארגון הבריאות "כללית", שבבעלותה נמצאים רוב בתי החולים הציבוריים במדינה. ארגון כללית, אשר משתמש במוניטורים על מנת לאסוף מידע על חולים המטופלים בה, חסמו את האפשרות להשתמש בחיבור אינטרנט אלחוטי בין המוניטור לבין מערכת ה-EMR, עקב החשש שהחיבור לרשת אלחוטית יפתח דלת לגישה זדונית של תוכנות אל תוך רשת בית החולים. החיבור האלחוטי לרשת של המוניטורים יקל בצורה משמעותית על החולים והרופאים כאחד משתי סיבות. ראשית, מאחר ועל סביבת הטיפול של כל חולה להיות סטרילית, כלומר נקייה מחיידקים, ה"אל-חוטיות" של המוניטור מקל על שמירה אופטימלית של סטריליות אזור הטיפול.   
שנית, מוקדי טיפול בחולים הינם ברובם מקומות פעילים שבהם אנשים מתרוצצים, מועברים חולים ומכשירי טיפול ממקום למקום. השימוש ב"אל-חוטיות" של המכשיר מאפשר תזוזה ומעברים פשוטים יותר ומשפרים את איכות הטיפול מצד החולה והמטפל יחדיו.*

*מנהלי מערכות ממוחשבות ואבטחת מידע ישתמשו בכלי, אשר יציג בצורה גרפית ואינטואיטיבית את מצבם הביטחוני של המוניטורים (כמה פעמים חדרו אליו אם בכלל, אליו נתונים שונו ומתי, וסוג התכנה הזדונית וצורת ההתקפה שבה הותקף המוניטור. יהיה ניתן גם להזעיק עזרה במידה והכלי/מטפל מבחין בבעיה שלא מצליחים לפתור בעזרת הכלי.)*

2.3 אילוצים עיקריים

**הגבלות ואילוצים עיקריים שצריך לקחת בחשבון בזמן עיצוב המערכת - אילוצי חומרה, סביבת ריצה, זמן ריצה וכו'.. (למשל – "המערכת דורשת חיבור לאינטרנט" / "המערכת צריכה לתמוך במספר רב של מערכות הפעלה" / "המערכת צריכה לתמוך במספר משתמשים רב")**

* *על המערכת לתמוך במספר מוניטורים רב*
* *המערכת דורשת מוניטורים אשר יחוברו לאנשים*
* *המערכת דורשת חיבור למערכת ה-EMR*
* *המערכת דורשת חיבור לאינטרנט*
* *המערכת צריכה להכיר במספר רב של תכנות זדוניות על מנת להגדירם בפני המשתמש*

2.4 הנחות ותלויות

**כל הנחה שיש לנו לגבי המערכת וסביבת הריצה שלה, ששינוי שלה עשוי לגרום לשינוי באפיון ובעיצוב - לדוגמא "המערכת תרוץ בסביבת לינוקס" זו הנחה המשפיעה על אפיון ועיצוב המערכת. אם נשנה את זה בהמשך נצטרך לעבור שוב על המסמך ולשנות את אפיון ועיצוב המערכת בהתאם (זה שונה מהסעיף הקודם- אילוצים זה לא משהו שיכול להשתנות, זה משהו שנקבע בתחילת העבודה ומשפיע רק על האפיון הראשוני). אל תתנו להנחות הללו להגביל אתכם בהמשך (אם תגלו שלמשל עדיף בסוף להריץ את השרת המרכזי מעל וינדוס – עשו זאת).**

**~ספציפיקציות שאנחנו צריכים לדון בהן~**

**2.5** סיקור מצב השוק כיום (אופציונלי)

**במידה וידוע לכם על מוצרים קיימים כיום (אתרים, תוכנות, אפליקציות וכו') שנותנים פתרון דומה (גם אם חלקי) לרעיון שלכם - קשרו אליהם כאן או תארו אותם בקצרה. התמקדו באופן שבו הם פותרים או מתייחסים לסוגיות דומות לאלו שבחרתם, מה הפיצ'רים העיקריים שהם מציעים ובמה הם שונים מהמוצר שלכם.**

*מתוך סקר שוק, עולה כי אין כלי/תכנית אשר עונה על הצרכים שצוינו למעלה, או שנותנים פתרון דומה (למיטב ידיעתי). ישנם פורומים רבים אשר דנים בשאלת בטיחות השימוש בתקשורת אלחוטית ברשת, אך לפי הממצאים שלי, אין בשוק כיום כלי דומה לכלי שאותו אפתח, אשר מתייחסים לסוגיה אותה בחרתי.   
אמנם לא נמצאו כלים, אך עולה כי בהחלט ישנה מודעות לנושא בעולם הסייבר-רפואה. ישנן כתבות ומחקרים רבים אשר מעידים על היתרונות והחסרונות של שימוש בחיבור רשת אלחוטי בבתי חולים. ב22 לינואר 2016, הוצא ארגון ה-FDA (הראשות האמריקאית לאישור תרופות ומכשירים) מסמך אשר נותן הנחיות לבנייה נכונה של מכשור רפואי אשר מחובר לרשת אלחוטית באופן בטוח ככל האפשר.   
אך כאמור, יחד עם כל המודעות לנושא, מפורומים בין רופאים ומומחי סייבר, ועד אחד הארגונים המשפיעים ביותר על עולם הבריאות כיום, לא עלה בחיפושי כלי אשר מגן על מוצרים אלו.*

1. דרישות מפורטות- ימולא בהמשך בהתאם למחקר

החלק העיקרי והחשוב ביותר של מסמך האפיון. פרק זה יכיל את הדרישות המפורטות מהמערכת שינחו את מעצבי המערכת, המפתחים, והבודקים בהמשך. כל דרישה שתפורט בחלק זה צריכה להיות:

* מזוהה על ידי שם (או עדיף - מספר) באופן ייחודי
* מתועדפת (כלומר מה העדיפות שלה כלפי הדרישות האחרות)
* ניתנת לבדיקה
* נכונה ושלמה
* עקבית ולא מתנגשת עם דרישות אחרות

*שימו לב שישנם מספר סוגים של דרישות, כפי שמפורט בכותרות כאן:*

*יש להשקיע בחלק זה ולפרט את הדרישות בצורה ברורה ונוחה להבנה. יש לזכור שזה לא מסמך עיצוב- יש להמנע מתיאור מפורט מדי שמגביל את העיצוב הטכני (למשל – שפת תכנות) שיגיע בשלב מאוחר יותר של עבודתכם.*

*את הדרישות רצוי לחלק לקטגוריות הבאות:*

3.1 דרישות פונקציונליות

**תיאור של פיצ'רים ספציפיים במערכת. לכל דרישה פונקציונלית מומלץ לפרט:**

* **הסבר כללי**
* **קלט**
* **תהליך**
* **פלט**
* **טיפול בשגיאות**

*ניתן (ואף רצוי) להציג את הדרישות הפונקציונליות בפורמט של* [*תרחיש שימוש (use case)*](http://he.wikipedia.org/wiki/%D7%AA%D7%A8%D7%97%D7%99%D7%A9_%D7%A9%D7%99%D7%9E%D7%95%D7%A9)*. בכל "נקודת זמן" של תיאור התרחיש יש לפרט את כל האפשרויות השונות שעומדות בפני המשתמש או המערכת, ומה יכול לקרות בכל התפצלות שכזו (שימו לב להתייחס גם למקרים שליליים, כמו שגיאות או נתונים לא מתאימים, ולא להניח שהמשתמש תמיד פועל בדרך שלה אנו מצפים)*

3.2 דרישות של ממשקים חיצוניים

**3.2.1 ממשקי משתמש** (למשל: GUI)

**3.2.2 ממשקי חומרה**

**3.2.3 ממשקי תוכנה** (אם התכנה מחולקת לכמה תוכנות שונות שצריכות לתקשר בניהן)

**3.2.4 ממשקי תקשורת (למשל תקשורת בין שר**ת ללקוחות)

3.3 דרישות לא פונקציונליות

*דרישות מהמערכת שלא מתבטאות בפיצ'ר ספציפי או בתהליך ספציפי שמתרחש במערכת אבל משפיעות על אופן עיצובה ומימושה, לדוגמא:*

**3.3.1 דרישות ביצועים (performance)**

**3.3.2 דרישות מהימנות (reliability)**

**3.3.3 דרישות זמינות (Availability)**

**3.3.4 דרישות אבטחה (security)**

**3.3.5 דרישות תחזוקה (maintainability)**

**3.3.6 דרישות ניידות (portability)**

3.4 דרישות בסיס נתונים

* *איזה נתונים יישמרו*
* *באיזה פורמט יש לשמור את המידע (DB / קובץ . ניתן לציין גם כמה אופציות)*
* *מה יכולות האחסון הנדרשות (נפח אחסון לדוגמא)*
* *מה רמת האבטחה הנדרשת*

3.5 דרישות נוספות

*כאלה שלא ידעתם לאיזה חלק הם שייכות*

1. בבליוגרפיה
2. *Luis Ayala, "Cybersecurity for Hospitals and Healthcare Facilities*

*A Guide to Detection and Prevention", APress, 2016*

1. *Symantec, "Symantec Industry Focus: Medical Device Security", 2016*

5. נספחים