שילוב הגנת סייבר בפרויקט

כנס אבטחת איכות

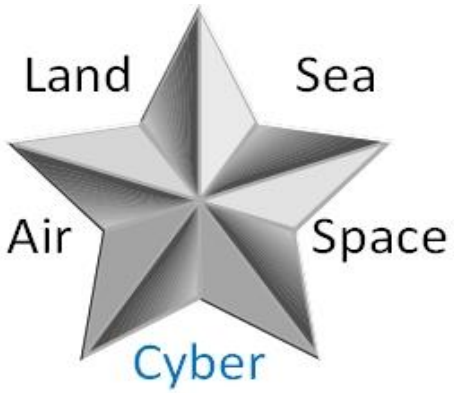
נובמבר 2015

נושאי ההרצאה

- תהליך הנדסת מערכת ברפאל
- תפקידי מהנדס מערכת סייבר
- הנדסת מערכת סייבר בכל אחד משלבי הפיתוח בשילוב הסיפור שלנו
- סיכום ומסקנות

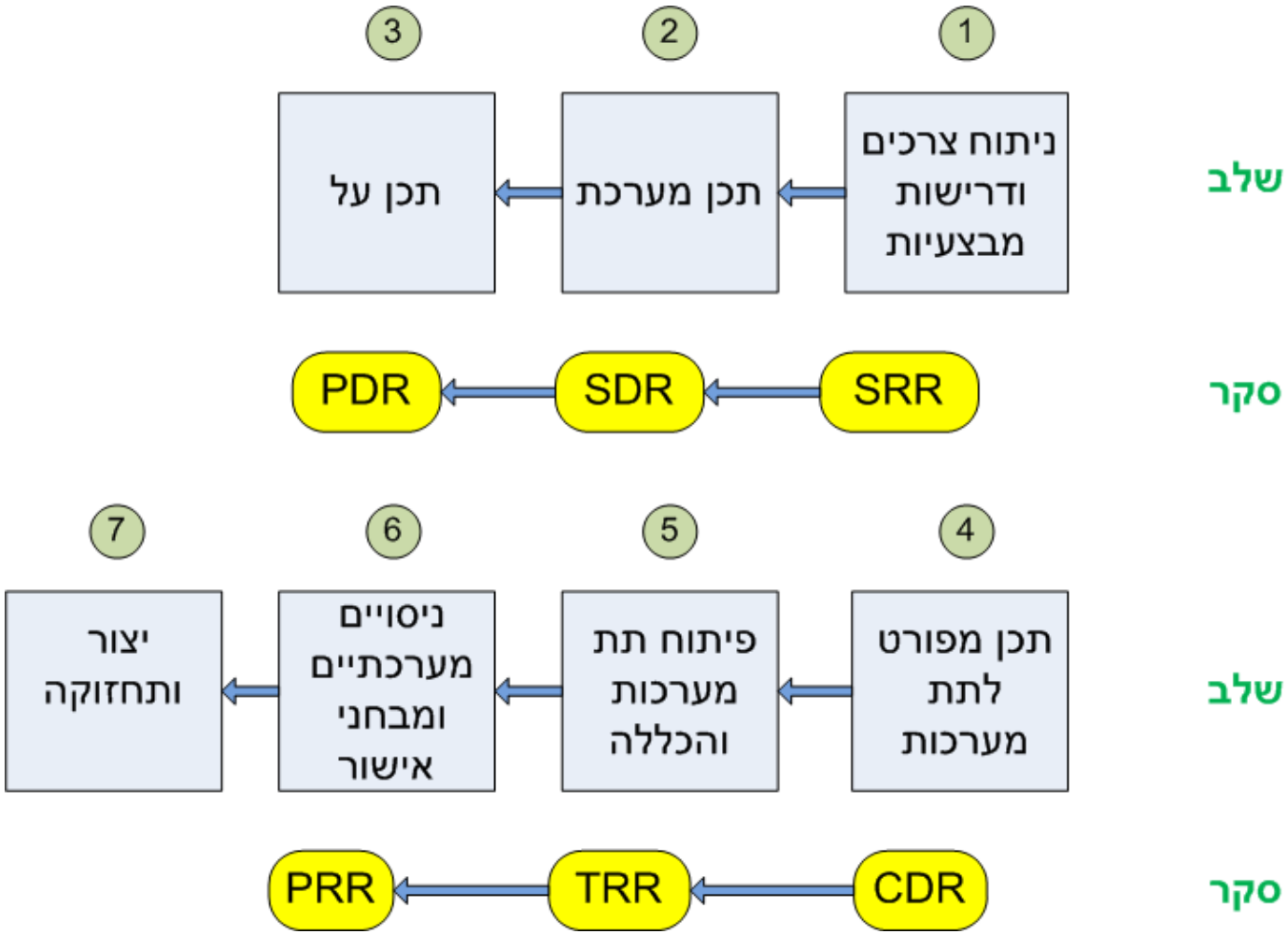
הנדסת מערכת

- פיתוח מערכת כולל דיסיפלינות שונות:
  - מכניקה, אוירונאוטיקה, פיסיקה, אלקטרוניקה, תוכנה, אלגוריתמים
- סייבר – דיסיפלינה חדשה
  מתפתחת ותופסת תאוצה בשנים האחרונות



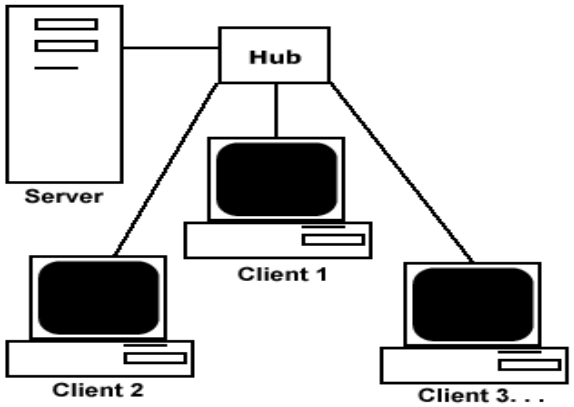
- מוגדרת כמימד לחימה נוסף
  אויר, ים, יבשה, חלל, וסייבר

תהליך הנדסת מערכת ברפאל



המערכת שלנו

- מערכת עתירת תוכנה בארכיטקטורת Client Server
- מידע מסווג



פעילויות הנדסת מערכת סייבר

❖שלב הגדרת דרישות מערכת

- ניתוח איומי סייבר
- הגדרת דרישות להגנה בפני איומי סייבר
- ניהול סיכונים

❖שלב תכן מערכת ותכן על

- הכנת חלופות טכנולוגיות
- ניתוח פתרונות תכן והמלצה
- הגדרת תהליכים תחזוקתיים נדרשים
- ניהול האיום השיורי

פעילויות הנדסת מערכת סייבר

❖שלב תכן

- מעורבות בתכן ממשקים
- מעורבות בדרישות ותכן של קבוצות חיצוניות – לדוגמא מומחי הקשחות

❖שלב מימוש

- לווי הפיתוח במעקב על עקרונות קידוד מאובטח
- השתתפות בסקרי קוד
- ממשקים עם קבוצות עבודה חיצוניות

פעילויות הנדסת מערכת סייבר

❖שלב בדיקות

- כתיבת מפרטי בדיקות סייבר
- אחריות על ביצוע הבדיקות
- ניהול פעילות מול צוות אדום

ניתוח איומי סייבר

- זיהוי הגופים המאיימים על המערכת ויכולותיהם

National Governments, Terrorists, Industrial Spies and Organized Crime Groups, Hacktivists

ניתוח תהליכי המערכת וממשקיה מהיבט הסייבר וניתוח סיכוני הפגיעה.

- ניתוח של כל אורחות החיים של המערכת : תפעול ,אימון , תחזוקה מהיבט הסייבר
- מערכת שלנו

- ניתוח האיומים בוצע במשותף ע"י מהנדס מערכת סייבר ומהנדס המערכת
- הלקוח לא היה שותף לתהליך הניתוח .השתתף בסקר

הגדרת דרישות סייבר

- הגדרת דרישות הנותנות מענה לאיומים
- ביצוע עקיבות בין הדרישות לאיומים
- הגדרת הדרישות מתבססת על תקנים
  לדוגמא : תקן מלמ"ב לדרישות בטחוניות
- דוגמאות לדרישות מהמערכת שלנו

– דרישה להזדהות נוספת לפני ביצוע פעולות מסוימות

– דרישה לשמירת לוג .רק לאפליקציה אפשרות כתיבה ללוג .מניעת אפשרות למחיקה או שינוי לוג.

– דרישות לפעילויות תחזוקתיות – הפעלת סריקת AV בתדירות נדרשת

ניהול סיכונים

- עדכון טבלת הסיכונים הפרויקטלים בסיכונים הנובעים משילוב הסייבר בפרויקט.
- דוגמאות
  - דרישה שאין פתרון טכנולוגי מוכח המיישם אותה
  - דרישה העלולה לפגוע בביצועי המערכת
  - דרישה העלולה לפגוע בתחזוקתיות המערכת
  - דרישה העלולה לפגוע באמינות המערכת

דוגמא

- דרישה להזדהות חזקה ע"י סיסמא + כרטיס חכם

השפעה

- מסרבל את המערכת – דורש יכולת נוספת של הפקת כרטיסים חכמים
- סיכון שמפעיל יגיע ללא הכרטיס החכם– פגיעה בזמינות

החלטה

- הזדהות ע"י סיסמא + ביומטרי

תובנה

- יש לבחון את השפעת דרישות הסייבר על דרישות אחרות כגון: תפעול, תחזוקתיות

דוגמא

- דרישה לבדיקה עיתית ע"י אנטי וירוס

השפעה

- קיים סיכון שעצם הרצת האנטי וירוס תשבש את המידע

החלטה

- שימוש בפתרון AV שמבטיח אי שינוי של המידע הנסרק

שלבי תכן מערכתי ותכן על

- הכנת חלופות טכנולוגיות לפתרונות
- המלצה על פתרונות תכן שנותנים מענה לדרישות
  - פתרונות מדף
  - פתרונות יחודיים לפרויקט
- דוגמאות
  - תוכנת מדף לחסימת התקניDLP
  - תוכנת מדף לניטור תהליכים

שלבי תכן מערכתי ותכן על

דוגמא

- דרישה להקשחת מערכת הפעלה - הפתרון המומלץ: שימוש ב GPOשלActive Directory

השפעה

- לא הכרנו את המשמעות של עבודה עם AD במערכת קטנה. ברפאל נסיון רק במערכות מיחשוב גדולות
- דורש ידע system ברמה גבוהה

שלבי תכן מערכתי ותכן על

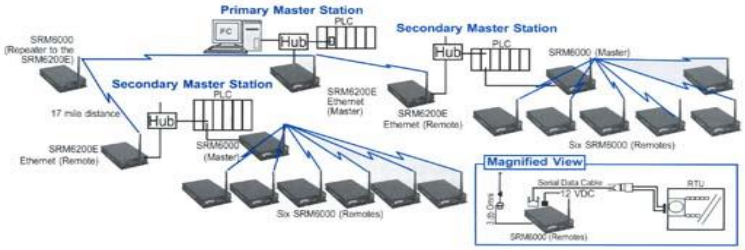
תובנה

- מהנדס מערכת סייבר חייב להכיר לעומק מנגנוני תכן עליהם הוא ממליץ ולהבין את המשמעות על לו"ז/עלות/זמינות
- כל פתרון שאינו מוכר חייב להבחן כדי להבין את השלכותיו על כל מחזור החיים מהפיתוח ועד לתחזוקה

שלב תכן

בשלב זה מצטרפים לתכן וישום מנגנוני הסייבר מומחי תוכן נוספים:

– מומחי הקשחת מערכת הפעלה



– מומחי תקשורות

– מומחי קריפטוגרפיה

שלב תכן

- ממ"ע סייבר מעורב בתכן ובסקרי התכן של כל הפתרונות שנבחרו
- ממ"ע סייבר אחראי על הגדרת דרישות לקבוצות החיצוניות (הקשחות) ומעורב בתכן ובסקרי התכן

דוגמא

- בקרת התקנים תאפשר חיבור client מזוהים
- בבקרת ההתקנים הוגדר שמאופשר כרטיס תקשורת מסוג מסוים

השפעה

- חיבור Client עם כרטיס תקשורת מסוג אחר מנעה תקשורת

שלב מימוש

- ממ"ע סייבר אישר את המדריך לכתיבת קוד מאובטח
- ממ"ע סייבר ביצע סקרי קוד לקטעים רלוונטיים
- ממ"ע סייבר השתתף בהחלטות ודיונים רלוונטיים – החלטה על ממשקים, הפרדה למתודות וחלוקת הקוד בין רכיבי המיחשוב

שלב בדיקות

- הבדיקות נכתבו בחלקן ע"י אנשי התוכנה ובחלקן ע"י ממ"ע סייבר.
- ממ"ע סייבר בצע את הבדיקות הרלוונטיות
- לא בוצעו בדיקות ע"י צוות אדום

"I don't know who those Cybers are, but I'm ready for their attack!"

סיכום ומסקנות

- דרישות סייבר מתנגשות לעיתים עם שיקולי אמינות ,תפעול נוח ,תחזוקתיות.
  נדרש להקפיד על איזון מתמיד לכל אורך הפרויקט
  מהנדס מערכת ראשי חייב להיות מעורב ולהביא את כל השקולים האחרים
- יש להתייחס לסייבר כמרכיב חשוב אך לא המרכזי במערכת
- נדרשת הבנה טובה של הפתרונות המוצעים והשפעתם על המערכת .
  אין לשלב אוטומטית Best Practices

סיכום ומסקנות

- לשילוב סייבר יש השפעה משמעותית על התוכנית בתכולות ,סיכוני לו"ז ועלות ,ביצועים
- יש להתיחס למרכיבי הסייבר במערכת כלשאר המרכיבים בהיבטי ניהול פיתוח) סקרים ,ניהול תצורה(
- למהנדס מערכת סייבר אחריות ותפקיד לאורך כל חיי הפרויקט כולל מימוש ,בדיקות ותחזוקה.
תפקידו אינו מסתיים בהגדרת הדרישות ובתכן על

סיכום ומסקנות

- תובנות מהפרויקט יושמו בתהליכים ומסמכים בחברה:
  - פרק סייבר במדריך הנדסת מערכת
  - מדריך תהליכי להנדסת מערכת סייבר
  - מדריכי קידוד מאובטח
  - הכשרות לקידוד מאובטח

שאלות???


"Sorry, your password must contain a capital letter, two numbers, a symbol, an inspiring message, a spell, a gang sign, a hieroglyph and the blood of a virgin"