SYSTEM EVALUATION AND ASSURANCE

פרק 26

שם : עזאיזה אדם

הקדמה

וידוי :

וידוי בא לענות על השאילה האם המערכת שייצרנו עונה על הדרישות שלה היא פותחה ,האם במקרה שמומחים מרביצים למערכת מספיק, המערכת תישאר חזקה ויציבה ועמידה ?

הערכה :

איך אנחנו יכולים לשכנע הקהילה, המנהל, הלקוחות שהמערכת באמת עושה את מה שהיא אמורה לעשות, ועובדת היטב.

וידוי ASSURANCE

הגדרה : הסיכוי לכך שהמערכת תיפול בדרך כלשהיא .זה תלוי בכמה גורמים מהם :

1- התהליך שבוא פותחה המערכת

2-מהות האנשים או הצוות שפיתחה את המערכת.

3-פרטים טכניים ,כמו האם השתמשנו באמצעים פורמליים ,כמה שגיאות השתלנו בכוונה לתוך המערכת כדי לראות כמה מהם נתפסו ע"י הבודקים .

למה בעצם צריכים לוודאות

-תמריצים הם קריטיים, אם אנשים לא רוצים להגן על המערכת ,קשה לשכנע אותם . אנשים הם החלק הקריטי ביותר של הסביבה שבתוכה מדיניות האבטחה צריכה להיות מוגדרת.

-מדיניות, לעומת שהיא מוזנחת לפעמים לוודות שהמערכת כן עושה והולכת על המדיניות שנקבעה אליה, יש הרבה מקרים שנתקלים הגנה על הדברים הלא נכונים , או הגנה על הדברים הנכונים בדרך הלא הנכונה.

-מימוש, נתן את הפונקציונליות ואת כוחם של המנגנונים המוסכמים, האם המוצר פועל בצורה נכונה.

USABILITY שימושיות

בתהליך הוודאות, לא לוקחים בחשבון להסתכל על שימושיות המערכת שיכולה להוות נקודת תורפה במערכת.

וידוי פרויקט

-וידוי כתהליך דומה מאוד לפיתוח של קוד.

-כמו שבאגים נמצאים בקוד שמפתחים, ובמפרט, באגים יכולים להופיע גם בשלב הבדיקה של המערכת.

-לכן, וידוי יכול להיות תהליך חד-פעמי, או להיפך, תהליך הערכה רציף.

-דוגמא, האנטי ווירוס שאפשר שתשתמש בתהליך רציף כמו Spiral Model, וגם בתהליכים חד פעמיים.

-מאגר ה-Malwares שרוצים לעשות עליהם נסיגה זה תהליך רציף.

-כאשר רוצים להוסיף טכניקות חדשות ורוצים לבדוק אותם, זה חד-פעמי.

בדיקות אבטחה

בדיקת אבטחה מסתמכת על

- 1-קריאת תיעוד המוצר
- 2-בחינת הקוד
- 3-ביצוע מספר בדיקות (tests)

תהליך בדיקת אבטחה :

- בדיקת פגמים אדריכליים .
- -בדיקת פגמים בעיצוב .
- -פגמים פחות נפוצות , כמו בדיקת מפתחות קריפטוגרפים חלשים , מייצר מספרים אקראיים חלש וכו' .

אמצעים פורמליים

-טכניקות לעיצוב מערכות שמשתמשות בהוכחות מתמטיות בנוסף לבדיקות בכדי לוודא התנהגות נכונה של המערכת.

-תעסוקה צבאית מחייבת להשתמש ב ORANGE BOOK ו- COMMON CRITERIA שבהסתמכות עליו משתמשים באמצעים פורמליים.

-אמצעיים פורמליים לא בהכרח ודאיות .

QUIS CUSTODIET IPSOS CUSTODES

מי ישמור על השומר ?

-טעויות יכולות גם להתבצע ע"י אנשים שמייצרים את רשימת הבדיקות .

מה עושים :

1- לפנות לארגונים מתמחים להצהיר על המערכת כמערכת ללא תקלות.

2-זריקת שגיאות בכוונה לתוך המערכת , ולתת לבודקים לבדוק .

“The errors you don’t know about are distributed the same as the ones you do”

וידוי תהליך

-בשנים האחרונות, פחות הדגישו על המערכת ובדיקת המערכת

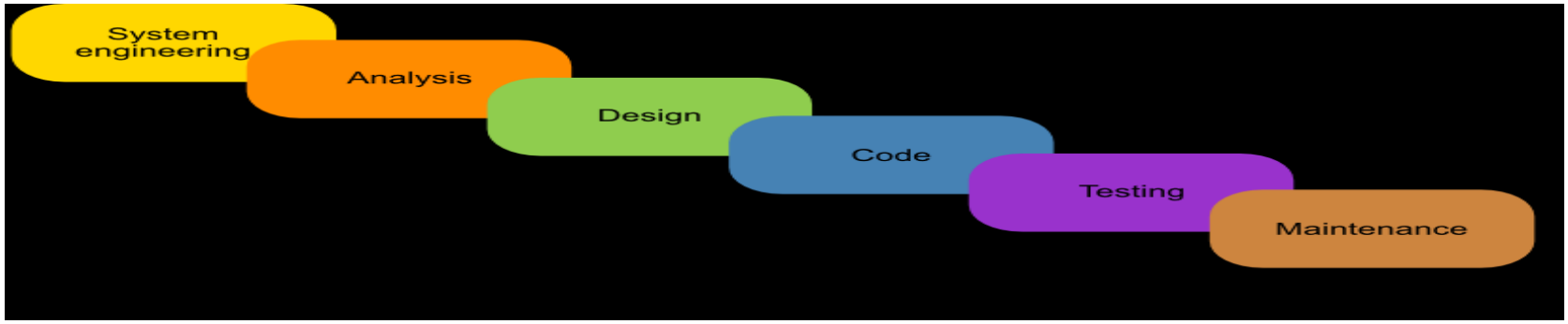
-הדגישו על מי בעצם פתח את המערכת .

-המודל של פיתוח מערכת יכול להשפיע .

-בשנות ה 1980 פיתחו ה- WaterFall Model

וידוי תהליך

-נתבונן במודל WaterFall שהוא מודל לפיתוח מערכות.



1-דרישות : דרישות מוצר, סכימה, כללים עסקיים .

2-עיצוב תוכנה.

3-תכנות.

4-בדיקות.

5-התקנה ותחזוקה.

וידוי תהליך

-מן הגורמים המשפעים גם הוא אם המפתחים אחראיים לתקן את הבאגים שעשו .

יתרונות WATERFALL MODEL:

- פשטות
- -שלבים אינם חופפים
- מודל זה עובד טוב בפרויקטים אשר דרישותיהם מובנים היטב .

חסרונות :

- -אם בשלב הבדיקה נמצא באג , קשה לחזור אחורה .
- -לא טוב עבור פרויקטים מורכבים מאוד .
- -לא מתאים לפרויקטים מתמשכים .

זה גרם למתכנתים לא לתת חשיבות באגים ולתת לבודקים לתקן , וזה גרם לאורך הזמן לצניחות באיכות ובייצור .

וידוי תהליך

-אנליסטים יחסו סכנת קרובת המוות ל- IBM כי היא השתמשה במודל של WATERFALL .

-לעומת זו , Microsoft השתמשה במדיניות שאומרת :

"אתה אחראי על תיקון קוד שכתבת "

שמכריחה העובדים לעשות את כל המאמצים בכדי לכתוב קוד נקי .

וידוי תהליך

-גורמים אחרים הלכו על מודלים להערכת האיכות של הקוד

Capabilty Maturity Model

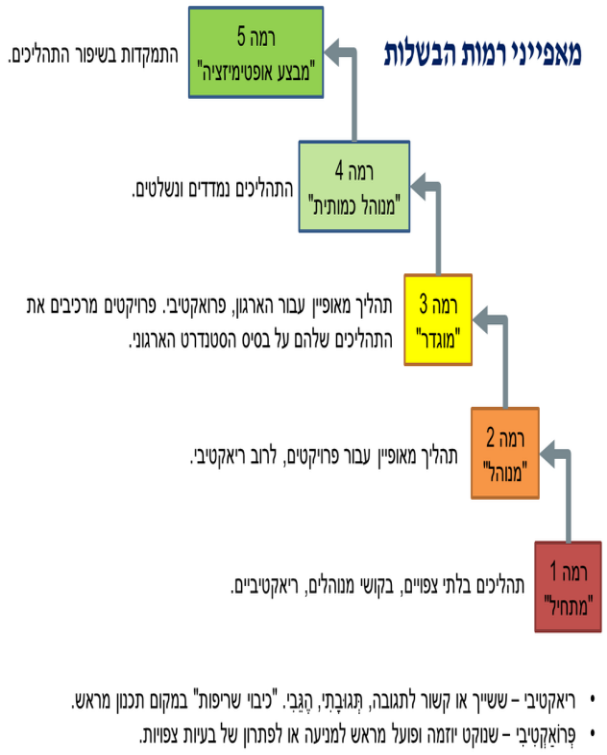
מודל שמספק רצף הדרגתי לארגונים ע"פ התהליכים שלהם בפיתוח מערכות.

ואז :

– יכולת היא תלויה בצוות ולא במפתחים בודדים .

-מפתחים מתחילים יכולים להיות שונים בסגנוני פיתוח, עיצוב קוד וכתיבת הערות, קצב עבודה .

-תפקיד המנהל הוא לנהל את כל זה ולהסכמה על שיטות עבודה ולתאם ביניהם.



וידוי תהליך

ISO9001 : ISO הם סדרת תקני איכות בינלאומיים המוגדרים ע"י ארגון התקינה הבינלאומי ISO.

בארץ , האחראי על זה הם מכון התקנים הישראלי

מהות התקן היא שהחברה חייבת לתעד את התהליכים שלה לעיצוב, פיתוח, בדיקות, תיעוד, ביקורת ובקרת ניהול בדרך כלל.

צמיחת הוודאות

-האיכות של מוצר יכול להגיע לשיווי משקל אם הקצב שבו באגים חדשים שנמצאו על ידי שיפורי מוצר שווה לאחוז שבו באגים ישנים נמצאו והוסרו.

- ההסתברות p כך שלא למצוא באג אחרי t בדיקות סטטיסטיקות אקראיות נתון בנוסחה : $p = e^{-Et}$ כאשר E תלוי באחוז הקלט שאפשר להשפיע .
- -במערכות גדולות. P=k/t עבור k קבוע כלשהוא .
- זמן ממוצע בין נפילות מערכת :
  - If you want a mean time between failure of a million hours, then you have to test for (at least) a million hours‘

הערכה והבטחת אבטחה

ניקח דוגמא, נניח שיש לנו מערכות מאוד מסובכות כמו Windows Vista שיש בהם כמיליון באגים, כל אחד עם MEBF של 1,000,000,000 שעות.

יש לנו תוקף איב, ואיש אבטחה עבור המערכת אליס.

על אליס למצוא את הבאגים לפני איב כדי לתקן אותם.

איב יכולה לעשות 1000 שעות של בדיקות בשנה, פרופ'.אליס יש לה את ה-source וכל הכלים שעוזרים לו לעשות מה שמקביל ל 100,000,000 שעות בדיקה בשנה .

אחרי שנה, איב מוצאת באג, ואליס מוצאת 10,000 באגים. יש לנו מיליון באג, לכן, הסיכוי לכך שאליס תפסה את הבאג של איב היא 1%. אחרי מאמץ גדול היא תמצא את הבאג של איב, ותעשה זאת בהסתברות די גבוהה אחרי 10 שנים. אבל איב תמצא 10 באגים אחרים בזמן זה .

במילים אחרות, לתוקפים אין מה להפסיד ,לכן ,יש להם יותר דינמיקה מאנשי האבטחה , וזו בעיה.

לכן, בא הנושא של **הערכת מערכת**

הערכת מערכת

-**הערכה** היא איסוף ראיות על כך שהמערכת עומדת, או לא עומדת, במטרה שנקבעה אליה.

-יש דאגה כאשר הצד שפתח את המערכת וזה שישתמש בה שונים .

-לפעמים הדאגה פשוטה :

-עיצוב אזעקה לסטנדרטים שנקבעו ע"י ביטוח,

ואושרו ע"י פקחים מקצועניים.

-מקרים מורכבים יותר :

-כאשר מנהלים שונים מתערבים, ספקי כרטיסי אשראי רוצים תעודת הערכה מהממשלה כדי למכור הכרטיסים לבנק, שרוצה לא לקחת על עצמו אחריות על הונאה .

הערכה ע"י צד מוסמך

-יש לנו מעבדות ומומחים שבודקים את המערכת.

-כרוך בתקציב קבוע של מאמץ(איש לשבועיים בתקציב של $15000).

-המעריכים יתחילו בתמונה כללית על "מה אמור המוצר לעשות ומה לא" .

-המעבדות מאשרות את המוצר, דורשות קצת שינויים או לא מאשרות .

הספר הכתום :

Trusted Computer System Evaluation Criteria (TCSEC)

סטנדרט של משרד ההגנה האמריקאית שמפרש דרישות להערכת מערכות מחשב .

התחיל בשנת ה -1983 , והוחלף ב CC אחר כך .

DAC AND MAC

Discretionary Access Control (DAC)

הוא סוג של אבטחת בקרת גישת שמעניק או מגביל את הגישה לאובייקט באמצעות מדיניות גישה שנקבעה על ידי קבוצת הבעלים של אובייקט.

מנגנוני DAC מוגדרים על ידי זיהוי משתמש עם אישורים שסופקו במהלך אימות, כגון שם משתמש וסיסמא.

DACsהוא שיקול דעת, משום שהבעלים יכולים לתת הרשאה על אובייקטים או גישה למידע למשתמשים אחרים.

במילים אחרות, הבעלים קובעים מתנגדים הרשאות גישה.

Mandatory Access Control (MAC)

הוא סוג של בקרת גישה שבה רק למנהל יש את האפשריות להגדיר את בקרת הגישה . המנהל מגדיר את מדיניות השימוש וגישה, שלא ניתן לשנות אותה על ידי משתמשים, והמדיניות תציין מי יש לו גישה אל האובייקטים והקבצים.

MACמשמש לרוב במערכות שבהן העדיפויות וההרשאות הן סודיות.

THE ORANGE BOOK

לפי TCSEC , אבטחת מערכת נערכת לפי 4 רמות , מרמה D עד רמה A1 כך שכל רמה מבוססת על הרמה שלפניה עם הוספת דרגות בטיחות .

רמה D מוגדרת להיות בטיחות מינימלית .

רמה C1 מוגדרת להיות הגנה מבוססת שיקול דעת .

רמה C2 מבוססת על C1 עם אבטחת בקרת גישה .

רמה B1 מוגדרת כאבטחת כותרת.

רמה B2 מוגדרת כאבטחה מורכבת .

רמה B3 מוגדרת כתחומי אבטחה .

רמה A1 מוגדרת כעיצוב מאומת .

THE ORANGE BOOK

C1 Systems: Discretionary Security Protection

-משתמשת ב-DAC.

-זיהוי ואימות משתמשים נדרש.

-הפרדה בין משתמשים ונתונים.

-תיעוד למערכת ומדריכים למשתמשים נדרש .

C2 Systems: Controlled Access Protection

בנוסף לאספקה כל התכונות הנדרשות ברמת C1, C2 דורשת:

1-ביקורת על משתמשים :המערכת יכולה לעקוב אחר מי עושה מה במערכת.

2-Audit trails: רשומות המספקות עדויות של הרצף של פעילויות שהתרחשו.

3-שימוש חוזר באובייקט :תכונה זו מוודאת כי כל הנתונים שנשארו בזיכרון, בדיסק, או בכל מקום אחר במערכת לא יהפכו לנגישים למשאבים אחרים אחר כך.

THE ORANGE BOOK

B1 Systems: mandatory access control

-הצהרה רשמית על מודל מדיניות האבטחה.

-MAC על מספר אובייקטים ומשתמשים.

-יש לסמן את רגישות המידע.

-מפרט על העיצוב.

B2 Systems: Structured Protection

-מודל מדיניות אבטחה מוגדר ומתועד באופן פורמלי.

-אכיפת DAC וMAC מורחבת לכל המשתמשים והאובייקטים.

-הפרדה בין אלמנטים עם הגנה קריטית ואלמנטים עם הגנה פחות קריטית.

-עיצוב ויישום שיאפשרו בדיקות רחבות יותר.

-מנגנוני אימות חזקים יותר.

-איש עם תפקיד מנהל מערכת(Administrator) נדרש.

-בקרות קפדניות יותר על המבנה.

THE ORANGE BOOK

B3 Systems: Security Domains

-מערכות שמקיימות את תכונות Reference Monitor

-מהנדסים מכוונים למזער את מורכבות(Complexity) המערכת.

-זיהוי ודיווח ותגובה אוטומטים בעת סכנה קרובה על המערכת.

-נהלי שיחזור מערכת.

-ביקורת על אירועי אבטחה רלוונטיים (Auditing Security Events).

A1 Systems: Verified Design

-פונקציונליות דומה למערכות B3.

-כל התהליכים נעשו באופן פורמלי ,כמו העיצוב, המפרט, הניהול, תהליכי ההפצה.

THE ORANGE BOOK

System	Example	
C1	Rare , earlier versions of Unix, IBM RACF.	
C2	This is one of the most common certifications. VMS, IBM OS/400, Windows NT, Novell NetWare 4.11, Oracle 7, DG AOS/VS II.	
B1	: HP-UX BLS, Cray Research Trusted Unicos 8.0, Digital SEVMS, Harris CS/SX, SGI Trusted IRIX.	
B2	Honeywell Multics, Cryptek VSLAN, Trusted XENIX.	
B3	The only B3-certified OS is Getronics/Wang Federal XTS-300.	
A1	These are the only A1-certified systems: Boeing MLS LAN, Gemini Trusted Network Processor, Honeywell SCOMP.	

THE ORANGE BOOK

-תהליך ההערכה מבוקר ע"י הממשלה.

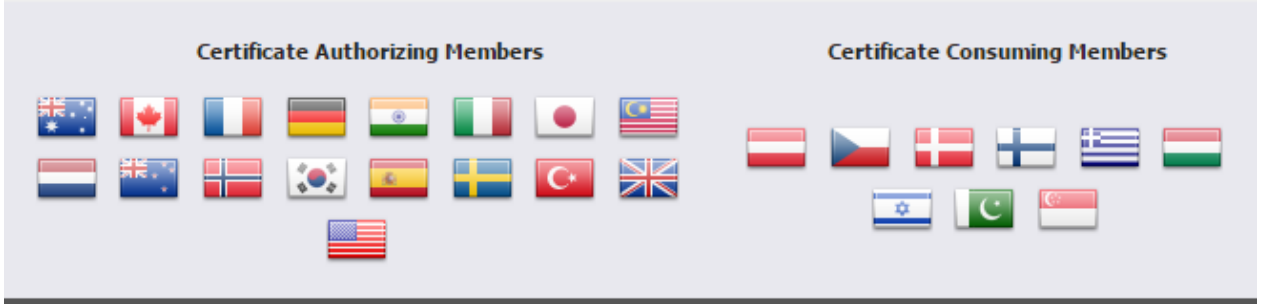
-היה לוקח שנתיים או יותר בכדי להצהיר על מערכת כמערכת הוערכה ,ואז מוצרים מוערכים היו דור אחר או שתיים מאחורי מוצרים נוכחיים ,ואז מוצרים אלה לא היו מתקבלים בשוק .

-אם הממשלה הייתה צריכה מערכת ,היא מוודאת אותה(בתהליך שייקח הרבה זמן), ואלה שפיתחו את המערכת ורוצים למכור הם כמתפללים אצל שער הממשלה עד שתסיים את הבדיקה ואז להחליט אם לקבל את המערכת .

THE COMMON CRITERIA

-הושג הסכם לבטל את ההערכה של כל מדינה בנפרד , ולהתאחד תחת תקן אחד .זה נגמר בשנת 1995 , והמודל האירופי ניצח עמיתו ,המודל האמריקאי והקנדי .

-כיום , יש הרבה מדינות מדינות חתמו שהן תומכות בסטנדרט



-כל ההערכה נעשתה במודל האירופי שנקרא ITSEC

ITSEC: Information Technology Security Evaluation

a system that was developed by a number of European countries .

THE COMMON CRITERIA

-יותר דינמי וגמיש מהספר הכתום.

-הספר הכתום הוא תקן מגביל , השוק יכול לבקש ולקבוע שילובים של תכונות אבטחה שלא מתאימות לאחד מן רמות הספר.

-נוצר הצורך לעבור לתקן חדש שהוא ה CC , המערכת מוערכת מפני Protection Profile.

מושגים והגדרות

-יעד ההערכה : (Target Of Evaluation TOE)

המערכת או המוצר עם התיעוד והמדריך שקשורים אליה שרוצים להעריך .

-יעד האבטחה : (Security Target ST)

סט של דרישות אבטחה ומפרטים לשמש כבסיס להערכה של ה- TOE.

-פרופיל הגנה : (Protection Profile PP)

סט של תכונות אבטחה ודרישות של אבטחת מערכת העונים לצרכי לקוחות ספציפיים.

-רמת וידוי והערכה (Evaluation assurance level EAL)

דירוג שמשקף את דרישות האבטחה שקיימה המערכת במהלך ההערכה.

SECURITY TARGET

ה ST של מערכת/מוצר מכיל :

-סוג המערכת .

-למשל Windows XP , הוא מוצר רב משימות, רב משתמשים, רב מעבדים.

-תיאור המערכת.

-Windows XP יש לו כמה גרסאות, ותיאור על כל גרסה.

-תכונות המערכת.

-התכונות המנהלתיים, תכונות אבטחת הרשת.

- שירותים ביטחוניים שמספקת המערכת

-Security Audit, I&A, User Data Protection, Crypto-protection

SECURITY TARGET

סביבת האבטחה:

-איומים אפשריים על המערכת :

-משתמש לא מורשה עלול לקבל גישה לנתונים עקב נפילת המערכת.

-מדיניות אבטחה ארגוניים :

-למערכת חייבת להיות את היכולת להגביל את היקף ההרשאות לכל משתמש.

מטרות ביטחוניות: מציעה איך להתגונן מפני האיומים, ואיך ליישם את המדיניות.

- TSFמחייבת להבטיח שרק למשתמשים מורשים יש את הגישה ל TOEו המשאבים שלה.

פרופיל הגנה

-קיימות היום הרבה פרופילים להגנה, יש ששייכים למערכות הפעלה, מכשירי סלולר, חומות אש, וידוי וזיהוי (Authentication and Certification) וכו' .

-PP_MD_v2.0, PP_GPOS_v3.9,CPP_FW_V1.0 .

-לפרופיל הגנה יש דרישות פונקציונליות, כמו :

1-תמיכה בהצפנה.

2-זיהוי ואימות.

3-ביקורת על האבטחה(Security Audit) : כמו –Monitoring,דיווח על אירועים ביטחוניים.

4-להגן על מידע המשתמשים.

-לפרופיל הגנה יש דרישות וידוי על האבטחה, כמו :

1-הערכת פרופיל הגנה : להראות שפרופיל ההגנה מושלם ועקבי.

2-בדיקות : לוודות שהבדיקות כיסו כל המקרים, עומק הבדיקה.

3-לוודות ששלב ההתקנה ואתחול המערכת בוצעו כהלכה.

אפשר למצוא פרופילי הגנה קיימים באתר :

https://www.commoncriteriaportal.org/pps/

האינטרסים של בעלי העניין

	Consumers	Developers	Evaluators
Part 1: Introduction and General Model	Use for background information and reference purposes. Guidance structure for PPs.	Use for background information and reference for the development of requirements and formulating security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
Part 2: Security Functional Requirements	Use for guidance and reference when formulat-ing statements of require-ments for security functions.	Use for reference when interpreting statements of functional require-ments and formulating functional specifications for TOEs.	Use as a mandatory statement of evaluation criteria when determining whether a TOE meets claimed security functions.
Part 3: Security Assurance Requirements	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

EVALUATION ASSURANCE LEVELS

Level	Description	Assurance
EAL 1	Functionally tested	Low
EAL 2	Structurally tested	
EAL 3	Methodically tested and checked	
EAL 4	Methodically designed, tested, and reviewed	Medium
EAL 5	Semiformally designed and tested	
EAL 6	Semiformally verified design and tested	
EAL 7	Formally verified design and tested	Highest

כאשר מתחילים ב EAL1

שדורש בדיקת

פונקציונליות, עד EAL7

שדורש מעבר לבדיקות ,

אימות באופן פורמלי .

הרמה הכי נפוצה היא

EAL4

לעומת שיש כרטיסי

אשראי המשתייכים ברמה

EAL6.

מוצרים ורמת ההערכה שלהם

Product	EAL
VMware® ESXi Server 3.5 and VirtualCenter 2.5	EAL4+
Microsoft Windows Mobile 6.5	EAL4+
Apple Mac OS X 10.6	EAL3+
Red Hat Enterprise Linux Ver. 5.3 on Dell 11G Family Servers	EAL4+
Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 2008 Datacenter Edition	EAL4+ ALC_FLR.3
Oracle Enterprise Linux Version 5 Update 1	EAL4+

דוגמא

-נניח שיש לנו מערכת הפעלה Windows 7 שרוצים להעריך על ידי CC.

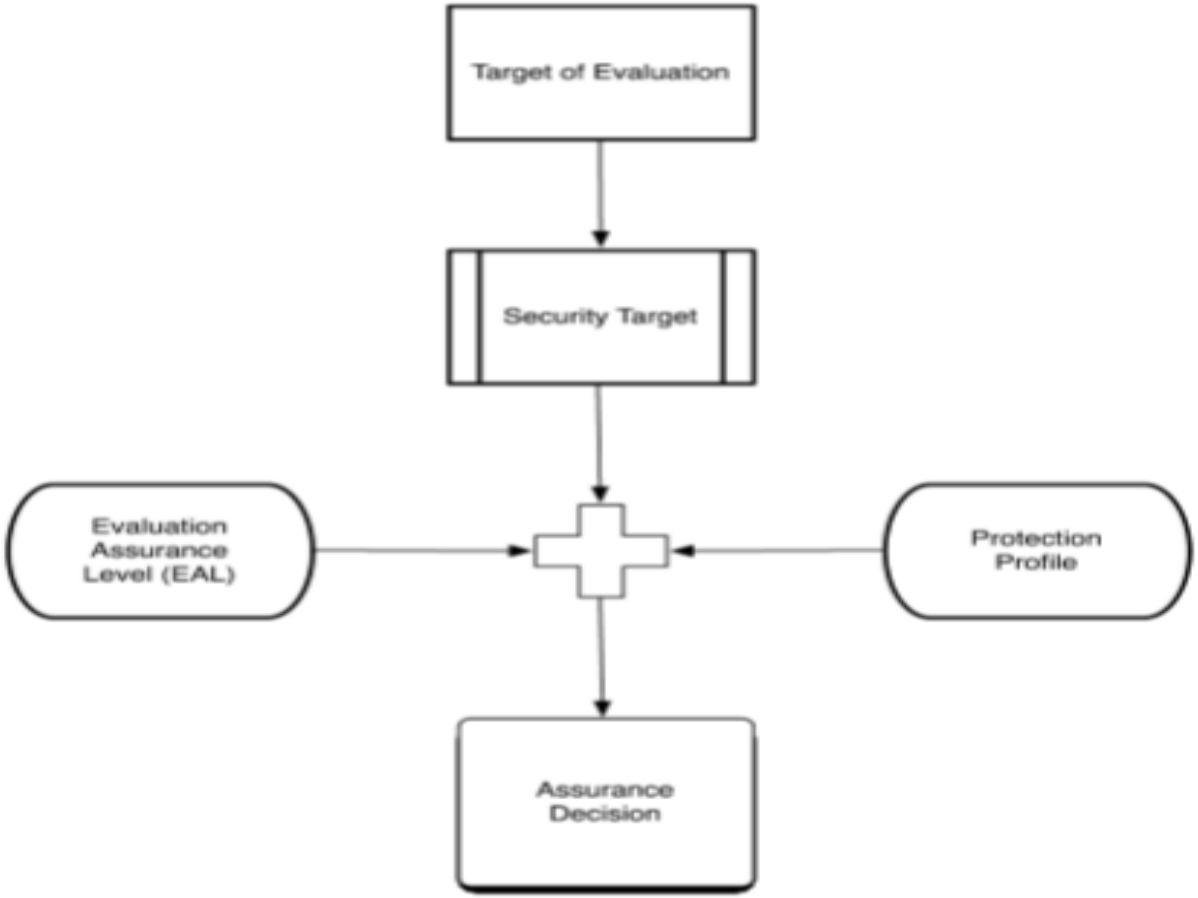
-מערכת ההפעלה משומשת למטרה כללית, תומכת בחיבור לרשת, בקרת גישה והפרדה ביו משתמשים.

-את פיתוח ה ST מסתמך על פרופיל ההגנה של

General Purpose Operating System Protection Profile.

-המעבדות מערכיות את ה- ST של – Windows 7 בייחס ל- GPOSPP על פי הקריטריונים של –EAL .

COMMON CRITERIA APPROACH



Operating System security – Trent Jaeger

סיכום

-וידוי של מערכת הוא תהליך מסובך, אך אנחנו חייבים אליו בכדי לאמת שהמערכת מממשת את יעד האבטחה שהיא אמורה לספק.

כדי לשכנע את האנשים שהמערכת עושה את עבודתה, זה לא תהליך פשוט,

-קיימות כמה שיטות להערכת מערכות

-דיברנו על הספר הכתום וה- Common Criteria

-המציאות מחייבת אותנו להשתמש ב – CC כדי לספק את צרכי השוק.

- ככל שהאנשים רוכשים ניסיון יותר , ויודעים מה הותקף ומה לא, ורוכשים ניסיון במנגנוני אבטחה ,עניין האבטחה ילך לטובה.

חיים הם מורכבים. הצלחה פירושה התמודדות עם המציאות .

התלוננות היא הדרך לכישלון.