ועדת האינטרנט הממשלתית מקיימת קורס אבטחת מידע במשרדי הממשלה.

בסיום הקורס יוצע למשתתפים קורס מתקדם וכן חברות בפורום חודשי המיועד לאחראים על אבטחת המידע במשרדים.

מטרת הקורס:

- להכשיר עובדים בעלי רקע וידע מתאים באבטחת מידע של רשתות מידע ותקשורת במשרדי הממשלה.
- העלאת המודעות לנושא אבטחת מידע בעידן האינטרנט, בה נחשפו ארגונים רבים לפריצות של גורמים מכל מקום בעולם.
- הצגת הדרכים לבניית מנגנוני אבטחת מידע החל מרמת מדיניות אבטחת המידע ועד הרמה הטכנית של בניית מערך אבטחת מידע על בסיס הטכנולוגיות החדשניות התופסות תאוצה במשרדי הממשלה.

מתכונת הקורס: הקורס יהיה בהיקף של 64 שעות, שמונה מפגשים בני שמונה שעות אקדמיות כל אחד (9:00-17:00). המשתתפים יתרגלו את הקורס בעיקר בין המפגשים ובמשך שעה בכל מפגש.

משתתפים: מספר המשתתפים בקורס מוגבל ל26-.

מיקום וזמן: מועד פתיחת המחזורים הקרובים מפורסם בלוח המודעות של אתר הוועדה.

הרשמה: ההרשמה לקורס תהיה על ידי פניה לאופיר בניהו מנהל מחלקת ההדרכה באוצר (טלפון : 02-5317210)

מרצים: את הקורס יעבירו מרצים בכירים העוסקים בנושא.

רקע נדרש: המשתתפים בקורס חייבים להיות בעלי ידע בסיסי נרחב בשימוש ברשת האינטרנט ועבודה ברשתות מחשב. מנהלים ביחידת המחשב ואנשי תשתיות האחראים על אבטחת המידע הממוחשב ביחידות מחשב של משרדי הממשלה

<u>הקורס לא מתאים למשתתפים שזוהי היכרותם הראשונית עם רשת האינטרנט ואו עם רשתות מידע ותקשורת</u>

הקורס מלווה בדוגמאות וסיפורים אמיתיים- Case Studies, בנוסף יינתנו הדגמות "חיות" לפריצות למערכות או גישה ללא הרשאה למערכות.

סילבוס הקורס :

1) אבטחת מידע- כללי:

- חשיבות המידע והסיכונים בחשיפתו לגורמים לא מורשים
- פשעי מחשבים - פריצות חיצוניות ושימוש של גורמים פנימיים לא מורשים
- סוגי הסיכונים בחדירה למערך המחשוב הארגוני
  - גניבת מידע
  - שתילה ועדכון מידע שגוי
  - הרס מידע
  - וירוסים
  - השבתת מערכות
- אבטחת מידע ברמת המחשב האישי
- אבטחת מידע ברשת תקשורת (WAN,LAN)
- אבטחת מידע ברשת האינטרנט / באינטרה-נט
- מנגנוני הגנה ואבטחת מידע
  - מנגנוני אבטחה פיזיים
  - סיסמאות והרשאות גישה
  - גיבויים
  - הצפנה
- מנגנוני שליטה ובקרה על מערך המחשוב
- הדרכים להתמודדות והגנה על המידע ברמת הארגון- בקרה, נהלים, אכיפה...

2) אבטחת מידע במחשב האישי:

- הסכנות וההגנה על המידע במחשב האישי
- מנגנוני הגנה ברמה הפיזית
- מנגנוני הגנה ברמת ה- DOS
- מנגנוני הגנה ברמת חלונות
- טיפול בוירוסים
- סיסמאות ברמת הדיסק, ספריות והקבצים
- מנגנוני הגנה בסביבת Office

3) אבטחת מידע ברשתות נפוצות:

Unix :

- כללי
- מבנה המערכת (Root ,Directories)
- תקשורת, סוגי עיבודים,משתמשים והרשאות
- היבטים בפתיחת המערכת לאינטרנט

NT:

- כללי
- מבנה הרשת וארכיטקטורה
- אכיפה ורישום
- ניהול דיסקים, גיבויים
- מושגים נוספים – RAS, Dial-up networking, CryptoAPI
- אבטחת מידע באינטרנט בסביבת NT

NOVELL:

- כללי
- מבנה המערכת (Root, Directories)
- תקשורת , עיבודים, משתמשים והרשאות
- אבטחת מידע ב- Intranetware

4) אבטחת מידע ברשתות מחשבים:

- אבטחת מידע ברשתות – כללי
- access ports, accountability
- רשתות LAN, WAN
- תווכי תקשורת- נל"נ, Ethernet, חיוג, ATM
- פרוטוקולי תקשורת (TCP, IPX...)

5) אבטחת מידע במסדי נתונים :

- בעיות ואתגרים בהגנה על מערכות מבוססות database
- פרצות ובעיות בהגנת נתונים ב- D.B – דרכי מניעה וסגירה
- ניהול הרשאות גישה
- מנגנוני בקרה ומעקב בגישה ל- D.B (Log file)
- מערכות מבוזרות- ניהול מערך אבטחה, Purging
- עקרונות ושיטות הצפנה

6) אבטחת מידע באינטרנט:

- כללי – בעיות ברשת האינטרנט
- בעיות בתוכנות/שרתי אינטרנט – FTP, EMAIL, IRC...
- אבטחת מידע בהיבטי האינטרה-נט – הרשת הפנים ארגונית
- שיטות הצפנה – אלגוריתמים- Des ..., מפתח ציבורי ופרטי
- פרוטוקולים מאובטחים
- התקני חומרה- Plug, כרטיסים, התקנים אחרים
- אבטחת מידע ב- JAVA
- אבטחת מידע בתוכניות הרצות על השרת (CGI)

.מדינת ישראל ,כל הזכויות שמורות / עמודים

- SET ,SSL
- Routing
- FireWall- ישום מדיניות הארגון
- אבטחת מידע ב- Browsers : Encryption, Verification, Java

7) היבטים משפטיים באבטחת מידע :

- חוק המחשבים ואחריותו של מנהל יח' המחשב כלפי החוק
- תקנות הגנת הפרטיות והשלכותיהן על אבטחת מאגרי המידע בארגון
- זכויות יוצרים בתוכנה, העתקות תוכנה ("גונבה") והשלכותיהן

8) סטנדרטים ותקינה:

- נוהל מפתח ואבטחת מידע
- הספר האדום והספר הכתום
- תקינה בינ"ל וישראלית בתחום

9) ניתוח צרכי אבטחת המידע בארגון :

- ☐ ניתוח סיכונים
- ☐ הגדרת מדיניות אבטחת המידע
- ☐ הגדרת דרישות ההגנה הפיזית
- ☐ הגדרת דרישות ההגנה הלוגית
- ☐ הגדרת דרישות ההגנה ברמת תשתית התוכנה
- ☐ הגדרת דרישות ההגנה ברמת האפליקציה
- ☐ הגדרת טבלת משתמשים (פרופילים, סוגים שונים)
- ☐ הגדרת טבלת הרשאות
- ☐ הגדרת רמת ההגנה הנדרשת
- ☐ הגדרת מנגנוני סיווג ומידור
- ☐ הגדרת דרישות ממנגנוני שליטה ובקרה (כלי ניהול, נהלים)
- ☐ דרישות כ״א לניהול (סוג/תפקיד)