פרק:	14	מערכות מידע
פרק משנה:	05	אבטחת מידע
נוהל מס':		14.05.16
גרסה:	1	מתאריך: 22.2.2017
עמוד	1 מתוך 3	עמודים

קרן קימת לישראל
KKL - JNF

קובץ נוהלי קק"ל

הגנה וטיפול בתוכנות מפגעות (וירוסים)

1. כללי

1.1 מערכת המידע המשמשת את הקרן הקימת לישראל, הינה רשת ענפה, אליה מתחברים משתמשים רבים, עובדים, וממשקים תפעוליים שונים באמצעות קווי תקשורת פנימיים וציבוריים, באמצעות עמדות מחשב קבועות ומחשבים אישיים ונישאים.

1.2 פריסה רחבה של משתמשים המחוברים למערכת באמצעות רשתות תקשורת שונות, אשר לא בהכרח מוגנות ומאובטחות, חושפת את מערכות המחשב של קק"ל בפני תוכנות מפגעות.

1.3 תוכנות מפגעות עלולות לגרום לנזקים חמורים במאגרי המידע, בתהליכים, באפליקציות ובכל דבר הקשור למערך המחשבים, כגון: שינוי מידע, האטת פעילות, מחיקת מידע והשבתה מוחלטת של מערך המחשוב.

1.4 לפיכך, קיימת חשיבות ראשונה במעלה לטפל במניעת כניסתן של תוכנות מפגעות אל תוך הרשת, איתור ומזעור הנזקים כאשר הן חודרות למערך המחשב.

2. המטרה

מטרת הנוהל לפרט הנחיות להגנת מערכת המידע של הקרן הקימת לישראל בפני תוכנות מפגעות (וירוסים).

3. תוכנה מפגעת (וירוס) - הסבר

3.1 תוכנה מפגעת הינה תוכנת מחשב היודעת, ללא התערבות מכוונת, לשכפל את עצמה למאגרי/קבצי מידע ובהמשך לפגוע בהם בדרכים שונות כמו: מחיקת מידע, האטת פעילות, מילוי זיכרון, שינוי מידע וכד'.

3.2 לתוכנה המפגעת קיימות ורסיות וסוגים שונים הפועלים באופן ייחודי על מערכות ההפעלה, זיכרון המחשב, תוכנות, אפליקציות וכד'.

3.3 זיהוי תוכנה מפגעת בעת תקיפת מערכת המחשוב, עשויה להתבטא בסימנים מעידים כגון:

3.3.1 אי יכולת להתקשר למערכת או להיכנס אליה;

3.3.2 נפילות פתאומיות של המערכת והפסקת תפקוד פתאומית של אפליקציות הפועלות במחשב באותה עת.

3.3.3 היעלמות קבצים או שינויים באופן שאינו ניתן להסבר.

3.3.4 העמסה בלתי מוסברת של זיכרון המחשב.

3.3.5 הופעת כתובת המודיעה על תקלה/וירוס.

3.3.6 התפרצות של תופעות לא ברורות ע״ג המסך.

3.3.7 תפקוד לקוי של המערכת וכיו״ב.

4. <u>שמירת המערכת מפני תוכנות מפגעות</u>

4.1 לצורך שמירת המערכת מפני תוכנות מפגעות, מותקנת במערכות השונות, בתחנות העבודה והשרתים, תוכנת הגנה ייעודית (אנטי-וירוס).

4.2 אגף מערכות מידע פועל לעדכן את הגרסה העדכנית הקיימת לכל חבילה, בכפוף להמלצות הספק והגורמים המקצועיים הרלבנטיים.

4.3 בעת השימוש במערכות מידע, ההנחה צריכה להיות היא שהאנטי וירוס מעודכן לקובץ חתימות האחרון שיש, ושמנוע האנטי וירוס הוא הגרסה האחרונה.

4.4 אין להסיר אנטי וירוס מתחנת עבודה או מחשב נייד ללא אישור אגף מערכות מידע.

5. <u>גילוי, טיפול ודיווח בעת הופעת וירוס בתחנת עבודה</u>

5.1 בכל גילוי וירוס בתחנת עבודה, יש לבצע פעולות לנטרול הנזק ולמנוע התפשטות הוירוס ברשת.

5.2 לצורך כך, מותקנת בכל תחנת עבודה תוכנת אנטי וירוס המנטרת את פעילות התחנה באופן שוטף.

5.3 עם גילוי וירוס בתחנה, מציגה תוכנת האנטי-וירוס הודעה מתפרצת על המסך המיועדת ליידע את המשתמש.

5.4 עם הופעת הודעה מתפרצת, על המשתמש לסגור את כל התוכנות הפעילות ולכבות באופן מסודר את המחשב.

5.5 על המשתמש להודיע טלפונית ומידית על גילוי ווירוס במחשבו למחלקת השירות ולהותיר את המחשב כבוי עד לבדיקתו ע״י טכנאי המחשוב של מחלקת השירות.

6. <u>פעולות מחלקת תשתיות</u>

6.1 מחלקת התשתיות יקבל נתוני קריאה ממחלקת השירות על מחשב המשתמש.

6.2 טכנאי מחלקת תשתיות יגיע אל המחשב החשוד ויבדוק את הסטאטוס של הווירוס או הקובץ החשוד כנגוע בווירוס.

6.3 סריקת החומר תיעשה באמצעות מנוע אנטי וירוס לפחות. במידת הצורך, יש לפרק את הדיסק קשיח ולהעבירו לצוות אבטחת מידע להמשך טיפול באמצעות חיבור הדיסק לתחנת הלבנה לטיפול בהסרת הוירוס.

חומר שנסרק וניימצא נקי, יוחזר למשתמש.

6.4 בכל מקרה, ייעשה כל מאמץ, לשמור על מרב החומר של המשתמש הנמצא על הדיסק הקשיח. יש לציין, כי באופן כללי, לא אמור להיות חומר חשוב על הדיסק הקשיח של המשתמש, אלא בשרתים באמצעות האפליקציות הייעודיות , דואר וספרית הקבצים ברשת.

6.5 עם סיום הטיפול תיסגר התקלה במערכת רישום התקלות.

6.6 בהמשך, יחובר המחשב מחדש לרשת והגורם המטפל ידווח על האירוע למנהל המחלקה.

7. <u>פעולות לעדכון המערכת</u>

7.1 על צוות תשתיות להיכנס מדי יום לכלי הניהול של התוכנה, לבדיקת מצב הווירוסים ולוודא שבכלי הניהול מוגדר כך שבעת התפרצות וירוסים (נקבע ע״פ כמות וירוסים ליחידת זמן) תשלח הודעת עדכון לתפוצה המתאימה.

7.2 במקרה שהאנטי וירוס אינו מצליח להתמודד עם הבעיה (כגון: וירוס חדש או מוטציה של וירוס קיים) יש להפעיל סריקה ע״י יותר ממנוע אנטי וירוס אחד וזאת על מנת לזהות את הקובץ הפוגעני.

7.3 את הקובץ שנוצר יש לשלוח לספק התוכנה, אשר נותן לקק״ל שירות בכל בעיות האנטי וירוס.

7.4 בדרך כלל, תוך שעתיים יגיע קובץ אשר פותר את הבעיה. במקרים מסוימים הוירוס משנה התנהגות (מוטציה) ואז ההתפרצות חוזרת על עצמה לאחר שעות או ימים.

7.5 בעת פתיחת הקריאה אצל ספק התוכנה, יש לקרוא לנציג מטעמו אשר אחראי ללוות את התהליך עד לפתרון.

8. <u>אחריות</u>

8.1 האחריות לביצוע הנוהל ויישומו, חלה על והגורמים המטפלים הפעלת מערכות המידע בקק״ל, וכל בעל תפקיד בקק״ל כנגזר מתוכן הנוהל.

8.2 האחראי לעדכון הנוהל ובדיקת התאמתו לצרכי הקרן הקימת לישראל יהיה מנהל הביטחון (מנב״ט) קק״ל בתיאום עם מנהל אגף מערכות מידע.

9. <u>תחולה ותוקף</u>

נוהל זה חל על כל עובדי הקרן הקימת לישראל והוא תקף מעת פרסומו.