## נוהל אנטי וירוס

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| זכויות יוצרים "התאחדות לכדורגל" ©מסמך זה והידע הכלול בו הינם הקניין הבלעדי של “התאחדות לכדורגל” ואינם ניתנים לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה במלואם ו/או בחלקם, במישרין, ו/או בעקיפין, ללא הסכמה מראש ובכתב של “התאחדות לכדורגל”.* מסמך זה מותר לשימוש פנימי בלבד.
* כל האמור בנוהל זה בלשון זכר או להיפך נעשה מטעמי נוחות ויש לראותו כאילו נאמר גם בלשון נקבה או להיפך.
* בדוק שהנך עושה שימוש בגרסה האחרונה של המסמך!
* בכל מקרה בו נדרש לערוך שינויים בנוהל זה, יש לפנות אל אחראי הנהלים ב”התאחדות לכדורגל”

נתונים כללים

|  |
| --- |
| ערך: בוריס קוגן  |
| בדק:  |
| אישר:  |
| סוג המסמך: מדיניות ונהלים  |
| תאריך פרסום המסמך: 01.02.2019 | תאריך תיקוף המסמך:  |
| סטאטוס המסמך: סופי  |

טבלת שינויים

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| תאריך שינוי | מהות השינוי | סעיפי השינוי | גרסה | גורם מאשר |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

 |

1. רקע:
	1. “התאחדות לכדורגל” (להלן "הארגון") מפעיל מספר מערכות מידע, אשר מכילות בין היתר מידע רגיש.
	2. תקשורת לא מאובטחת או מאושרת עלולות לגרום לנזקים חמורים לארגון, כגון: חשיפת מידע רגיש, העברת מידע לגורמים לא מורשים, שינוי לא מורשה של מידע, האטה של הפעילות ברשת ו\או של המחשב הנגוע, מחיקת מידע לא מורשית והשבתה מוחלטת של מערכות המחשוב ב”התאחדות לכדורגל” (להלן "הארגון").
	3. קיימת חשיבות ראשונה במעלה למנוע פגיעה במערך המחשוב בכלל וע"י מערוכת ההנהגה בפרט.
	4. לצורך עבודה שוטפת, יש צורך בהגדרת עקרונות מנחים לניהול ועדכון מערכות אנטי וירוס.
2. מטרה:
	1. להגדיר תהליכי עבודה בהתקנה, ניהול ועדכון מערכות אנטי וירוס.
	2. לנקוט באמצעי מנע על מנת להבטיח כי מערכות המידע של הארגון לא ייפגעו כתוצאה מהידבקות בתוכנות זדוניות.
3. מסמכים ישימים:
	1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
4. אחראי לביצוע הנוהל:
	1. מנהל אבטחת מידע והסייבר.
	2. אחרי ליישום - מחלקת תשתיות.
5. הגדרות:
	1. "נוזקה" - תוכנה זדונית אשר מטרתה היא לפגוע בשלמות, זמינות או אמינות המידע. הסוגים הנפוצים ביותר של נוזקות הם "ווירוס" או "סוס טרויאני".
	2. "ווירוס" - תוכנה זדונית שמטרתה להדביק קבצים אחרים על אותו מחשב ולנסות לגרום נזק ע"י הפעלת קובץ ההרצה (Payload) שלו, ע"י המשתמש.
	3. "תולעת" - תוכנה זדונית שמטרתה לגרום נזק לארגון ו\או למערכות בארגון ע"י גרימת עומסים, גניבת מידע ועוד. התולעת מפיצה את עצמה ברשת באופן עצמאי, לאחר ההידבקות.
	4. "סוס טרויאני" - תוכנה זדונית "מוסתרת", המגיעה בצורה של תוכנה לגיטימית, ולאחר ההתקנה ע"י המשתמש, היא מעבירה מידע חסוי לבעל התוכנה (פגיעה בסודיות המידע) או מאפשרת לתוקף דלת אחורית למערכת הנפגעת.
	5. "תוכנת אנטי-וירוס" - תוכנה אשר מטרתה היא לאתר את הנוזקות ולבצע סט של פעולות במטרה להודיע על הימצאות הנוזקה, ולנסות למחוק ולהסיר את התוכנה הזדונית, או לפחות למנוע את הפעלתה בצורה תקינה.
6. גוף הנוהל:
	1. כללי
		1. מקורות איום
			1. **מקורות חיצוניים**
				1. גלישה ברשת האינטרנט
				2. דואר אלקטרוני
				3. תוכנות מסרים מיידים
				4. תוכנות שיתוף (P2P)
				5. חדירה של פורצים
			2. *מקורות פנימיים*
				1. מחשבים ניידים
				2. סמארטפונים
				3. מדיה נתיקה
		2. עדכון מפני איומים ידועים בנושאי נוזקות
			1. מנהל הרשת או מי מטעמו יתעדכן באופן שוטף במידה הנודע לפרצות ידועות, מספקי הציוד או מאתרים המספקים שירותים אלו באינטרנט (שירותי מודיעין סייבר).
			2. כל עובדי אגף מערכות מידע בכלל, והעובדים האחראים על התפעול השוטף של תוכנות האנטי-וירוס בפרט, יעודכנו על ידו בכל מידע בעת נגיעה לתחומי הפעילות הנ"ל.
			3. בהתאם למידע זה, יבצעו מנהל הרשת וצוותיו שדרוגים או עדכונים, למערכות שבתחום אחריותם.
		3. זיהוי נוזקות
			1. ישנם אירועים אשר עלולים להצביע על הימצאותה של תוכנה מפגעת במערכות המחשוב:
				1. התרעה מתוכנת האנטי-וירוס על הימצאותו של וירוס (נוזקה) במערכת.
				2. פעילות רשתית מוגברת של המערכת אשר יכולה להצביע על ניסיון של הווירוס להפיץ את עצמו.
				3. תופעה לא מוסברת של תהליכים שרצים ברקע.
				4. האטה כללית בביצועי המחשב עקב פעילותו של הווירוס.
				5. תוספות לא מוסברות של קבצים מוסתרים ו\או לא מוסתרים במערכת.
				6. העלמות לא מוסברת של קבצים או ספריות שלמות במערכת.
	2. התקנה, ניהול ועדכון והפצה שרת אנטי-וירוס
		* 1. *התקנה בשרתים*
				1. בכל מחשב חדש, באחריות צוות תשתיות שבבעלותו השרת, להתקין את תוכנת האנטי-וירוס שמתאימה לשרתים, ולהוסיף את השרת לממשק הניהול המרכזי של תוכנת האנטי-וירוס בארגון.
				2. במידה ומתבצעת דריסה של מערכת ההפעלה וההתקנה היא לא על מחשב חדש, יש לבצע סריקה של כל הכוננים במערכת ובכך להבטיח שלא יעברו נוזקות מההתקנה הישנה לחדשה.
				3. בשרתים תוגדר תוכנת האנטי-וירוס כך שכל קריאה וכתיבה ותבצעו בבקרה של תוכנת האנטי-וירוס על מנת לפצות על כך שלא מתבצעת סריקה יום-יומית.
		1. ניהול
			1. *ניהול שרת האנטי-וירוס*
				1. יש לוודא ניהול ותחזוקה תקינה של שרת האנטי-וירוס.
				2. במידת הצורך, יש לבצע הקשחה של השרת.
				3. יש לוודא עדכון טלאים ועדכוני תוכנה (SP) לצורך שמירת עדכניות גרסאות מערכות ההפעלה.
			2. *ניהול אנטי-וירוס במחשבים*
				1. יש לקבוע סריקה יזומה של השרתים פעם בשבוע כאשר הדבר מתאפשר.
				2. במקרים מיוחדים, כגון שרת בעל נפח אחסון ענקי אשר סריקה יזומה שלו לא יכולה להתבצע בפרק זמן סביר, יש לפרק את הסריקה לחלקים כאשר כל חלק ייסרק בזמן אחר. כמו כן, יש לדאוג שכאשר יש חלון זמן אשר בו הסריקה יכולה להתבצע בשלמותה (כמו למשל בתקופה של חג בו החברה לא פעילה) תתבצע הסריקה.
				3. יש לבצע בדיקת כיסוי שבועית של תוכנת האנטי-וירוס בסגמנטים שונים של השרתים. במידה ונמצא שרת לא מנוהל, יש להתקין עליו את תוכנת האנטי-וירוס ולברר מדוע היא לא הותקנה עליון מלכתחילה (Root Cause Analysis).
		2. עדכון והפצה
			1. *עדכון והפצה במחשבים*
				1. כל עדכון שיוצא מיצרן תוכנת האנטי-וירוס יופץ לכל התחנות באופן מדורג, על מנת להבטיח הגנה מלאה מאיומים של נוזקות חדשות. מידה וישנה התפרצות חדשה של וירוס (נוזקה) באינטרנט, יש לבדוק מול הספק (צרן) האם יצאו או ייצאו עדכונים ספציפיים לווירוס זה ובמידה וכן יש להפיצו כמה שיותר מהר לתחנות העבודה בארגון.
				2. יש לעדכן את הגרסאות של תוכנת האנטי-וירוס תוך חודש ימים מיום הוצאתה.
				3. את קובץ החתימות, יש לעדכן ברמה היומית (במידת הישימות) או לפחות השבועית.
				4. יש לבצע בדיקה חודשית של כיסוי תוכנת האנטי-וירוס בסגמנטים שונים של תחנות העבודה ברשת הארגון, בכדי למצוא תחנות אשר לא מנוהלות ע"י ממשק הניהול המרכזי. במידה ונמצאו תחנות כאלה על צוות אבטחת המידע לחקור כיצד הותקנה תחנה ללא תוכנת האנטי-וירוס וללא וידוא שהיא אכן מנותרת.
	3. תיעוד ודיווח
		1. רישום פעילות
			1. תיעוד ודיווח על אירועי חדירות וירוסים או נוזקות אחרות יתבצע באופן אוטומטי במערכת (שרת האנטי-וירוס).
			2. כמו כן, יש לתעד את האירועים הקריטיים (נוזקות ברמת חומרה\קריטיות גבוהה) בהתאם לנוהל "ניהול אירועי אבטחת מידע".
				1. דו"ח אירוע אבטחת מידע.
				2. דו"ח פעולה מתקנת ומונעת.
	4. בקרה
		1. פעילות בקרה
			1. מנהל תחום אבטחת המידע בארגון יבדוק אחת לשנה את קיום הנוהל ויתקנו בהתאם להליך הפקת לקחים.
		2. פעילות מונעת - מודעות
			1. באחריות מנהל תחום אבטחת המידע בארגון לפעול להדברת המודעות בנושא התגוננות מפני וירוסים ותוכנות זדוניות אחרות.
			2. יש לתדרך את כל משתמשי המחשוב בארגון בנושא סוגים וזיהוי של תוכנות זדוניות והאפשרות למנוען.
			3. חשוב להבהיר את גודל הנזק ולהסביר את האחריות האישית של כל משתמש להגנה על מערכות המחשוב בארגון.
7. אכיפה
	1. כל עובד שימצא כי הפר את מדיניות זו עשוי להיענש על ידי הגורם הרלוונטי ב”התאחדות לכדורגל”, המחלקה או “התאחדות לכדורגל” עצמו.
8. תחולה
	1. המדיניות חלה על כלל עובדי “התאחדות לכדורגל” (ספקים, עובדי קבלן, יועצים, זמניים) ועובדים אחרים המחזיקים או מתחזקים מידע כלשהו של “התאחדות לכדורגל”.
	2. נוהל זה נכנס לתוקפו מיום פרסומו.
	3. מכניסתו לתוקף, נוהל זה מחליף כל נוהל קודם בעניין.