מדיניות עדכון מערכות המידע, רכיבי התקשורת ומערכות האבטחה הלוגיות בממשל זמין

גרסה 1.0

מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1.0	3.3.2016	אלעד פז	גרסה ראשונה

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	PMO	אופיר יהב	3.3.2016	(חתימה)
נבדקה ע"י	מוביל טכנולוגיות במערך סייבר ואבט"מ	אלעד פז	11.2.2016	(חתימה)
אושרה ע"י	מנהל תחום סיסטם	רונן אברהמי	4.2.2016	(חתימה)
אושרה ע"י	מנהל מערך סייבר ואבט"מ	אברהם זרוק	3.3.2016	(חתימה)

תוכן עניינים

1. כללי

1.1. ממשל זמין אחראי על אבטחת סודיות, שלמות וזמינות המידע (מידע פנימי של ממשל זמין ושל לקוחותיו) המאוחסן במערכות המידע של ממשל זמין.

1.2. ממשל זמין מחויב לספק את ההגנות המתאימות כנגד תוכנות זדוניות (Malware) כגון: Viruses, Trojans, Warms (וירוסים, טרויאנים ותולעים) וכו' היכולים להשפיע לרעה על אבטחת מערכות המחשוב ו/או המידע האגור בהן.

1.3. הטמעה אפקטיבית של מדיניות זו תגביל את החשיפה וההשפעה של איומים שונים הנובעים מתוכנות זדוניות נפוצות למערכות המידע ולרשתות התקשורת.

2. המטרה

2.1. קביעת מדיניות עדכון טלאי האבטחה/קושחות למערכות המידע של ממשל זמין (תחנות העבודה, השרתים, רכיבי התקשורת, יישומים ומערכות האבטחה הלוגית).

2.2. תיאור דרישות מנהל מערך סייבר ואבטחת מידע לשמירת טלאי האבטחה והקושחות העדכניים ביותר של מערכות ההפעלה בכל תחנות העבודה, השרתים, רכיבי התקשורת ומערכות האבטחה הלוגיות בממשל זמין.

3. הגדרות

3.1. **Patch (טלאי)** - פיסת תוכנה שנועדה לתקן בעיות ו/או לעדכן את תוכנת מחשב או נתונים התומכים בה.

3.2. **Firmware (קושחה)** - תוכנה המשובצת בהתקן חומרה, ומטפלת בתפקוד הרכיב.

3.3. **Trojan (טרויאן)** - תוכנת מחשב מזיקה המנסה לחדור למחשב תוך התחזות לתוכנה תמימה. תוכנה זו אמורה לבצע פונקציה רצויה אך למעשה מבצעת פונקציה זדונית.

3.4. **Virus (וירוס)** - קוד זדוני בדמות תוכנת מחשב החודרת למחשב ללא ידיעת המשתמש, וגורמת על פי רוב לפעילות לא רצויה העלולה לפגוע בתפקודו של המחשב או הרשת בה הוא ממוקם או לפגוע בשלמות, זמינות או סודיות המידע הנמצא עליו. וירוס עשוי להפיץ את עצמו למחשבים נוספים בדרכים שונות ובכך לשכפל ולהעצים את מטרתו.

3.5. **WARM (תולעת)** - תוכנת מחשב או מקטע מתוכנת מחשב אשר מאופיינת ביכולת הפצה עצמית (התפשטות) אל עבר מחשבים אחרים באמצעות רשת מחשבים. תולעי מחשב לרוב נושאות "מטען" זדוני בדמות וירוס ו/או מזיקות בצריכה גבוהה של רוחב פס.

3.6. **אפליקציה / יישום** – רכיב תוכנה המותקן על גבי מחשב (שרת או מחשב נייד/נייח).

4. אחריות ליישום המדיניות

4.1. **מנהל מערך סייבר ואבטחת מידע** - קביעת המדיניות ועדכונה מעת לעת.

4.2. **מנהל מערך ה-IT** - אחראי, אחריות ניהולית, על יישום המדיניות.

4.3. **מנהל תחום ה-SYSTEM** - אחראי, תפעולית, על יישום המדיניות ודיווח למנהל מערכות המידע.

4.4. **מנהל רשת אדומה** – אחראי על הפצת העדכונים השונים (מערכת הפעלה, תוכנה וקושחה) לתחנות העבודה (מחשבים נייחים ומחשבים ניידים).

4.5. **מנהל תחום אירוח** - אחראי, תפעולית, על יישום המדיניות ודיווח למנהל מערכות המידע.

5. תחולה

5.1. מדיניות זו חלה על כלל תחנות העבודה, השרתים, רכיבי התקשורת, יישומים ומערכות האבטחה הלוגית בבעלות ממשל זמין או מנוהלות על ידו. כולל מערכות המכילות מידע של לקוחות ללא קשר למיקומם הפיזי.

6. מחזור חיים של התקנת עדכונים/קושחות

6.1. <u>פגיעות חדשה</u>

6.1.1. ספק מודיע ללקוחות על גילוי פגיעות חדשה, או לחילופין, לקוח מגלה פגיעות חדשה במוצר. הפגיעות נבדקת על-ידי צוות אבטחת האיכות של הספק ולאחר מכן מפותח טלאי (או שינוי הגדרות) לצורך תיקון הפגיעות.

6.1.2. לתוכנות מסחריות נפוצות הספק מודיע על הפגיעות והעדכון/טלאי בהתאם. במקרים אחרים הספק יוצר קשר ישיר עם הלקוחות על-מנת להודיע להם על הסיכון/פגיעות ופעולה/ות שיש לנקוט.

6.2. <u>סקירה</u>

6.2.1. הודעת הפגיעות והפתרון (טלאי) המוצע על-ידי הספק נסקרת על-ידי הלקוח. במהלך מצב זה נבדקים נכסי המידע על מנת לקבוע האם פגיעות התוכנה קיימת באחד מנכסי מערכות המידע. ארגונים שונים בוחרים להשתמש בסורקי פגיעויות מבוססי רשת על מנת לזהות נכסים הדורשים תיקון (מבוצע באמצעות "סוכנים חכמים" המותקנים בנכסים).

6.2.2. לאחר גילוי קיום הפגיעות והתאמת העדכון/טלאי אושרה, מתחיל תהליך ניהול הסיכונים.

6.3. <u>הקצאה</u>

6.3.1. לאחר תהליך ניהול הסיכונים, יוקצה "בעל נכס" – הישות הבלעדית בעלת אחריות לשמירת סודיות, זמינות ואמינות הנכס. ישות זו תהיה אחראית על קבלת המידע הרלוונטי אודות הפגיעות ואפשרויות הטיפול בה.

6.3.2. בשלב זה מתחיל תכנון משאבי IT הכולל מנהלי מערכת, תמיכת תוכנה, מפתחים, בקרת איכות ואנשי רשת כמו גם ספקים שותפים.

6.3.3. פעולות לביצוע:

6.3.3.1. קבלת העדכון/טלאי.

6.3.3.2. הכנת חבילת העדכון להפצה.

6.3.3.3. תכנון לוח זמנים להפצת העדכון.

6.3.4. אישור להתקנת העדכון/טלאי יבוצע באישור בעל הנכס בלבד.

6.4. <u>השהייה</u>

6.4.1. בעל הנכס או מערכות המידע יכולים לבחור להשהות את התקנת העדכון/טלאי מסיבות שונות (לדוגמה: מניעת שינויים בעת העלאת גרסה חדשה) – מדובר בהשהיה בלבד, קרי, תבוצע בתקנה בעתיד.

6.4.2. השהיית עדכון דורשת אישור הנהלה כתוב, המפרט את קבלת הסיכון. מסמך הדחייה יתועד בהתאם לצורך ביקורות עתידיות.

6.5. <u>דחייה</u>

6.5.1. בעל הנכס או מערכות המידע יכולים לבחור בדחיית העדכון ולא להתקינו כלל בשל בעיות אינטגרטיביות וכו'.

6.5.2. דחיית עדכון דורשת אישור הנהלה כתוב, המפרט את קבלת הסיכון. מסמך הדחייה יתועד בהתאם לצורך ביקורות עתידיות.

6.6. <u>בדיקה</u>

6.6.1. שלב זה כולל בדיקה והטמעה של עדכון האבטחה ולכן דורש תשומות כוח אדם רבות שצריך לקחת בחשבון.

6.6.2. מעקב אחר ניהול השינויים הינו מרכיב קריטי בתהליך.

6.6.3. של בדיקת העדכון/טלאי ויישום הדרגתי של ההתקנה חשוב מאוד שכן קיימים עדכונים שלא ניתן להסירם לאחר התקנתם.

6.7. <u>סקירה חוזרת</u>

6.7.1. מטרת שלב זה הינה המשך הטמעת העדכון/טלאי לאחר החלטת הארגון להשהותו. קידום נושא התקנת העדכון/טלאי בסביבת הייצור מותנה באישור בעל הנכס ומערך ה-IT.

6.8. אימות

6.8.1. שלב זה מוודא כי העדכונים מבצעים את ייעודם. דבר זה נעשה באמצעות מוצרים שונים לאימות הטמעת העדכון/טלאי כדוגמת סורקי פגיעויות מבוססי רשת.

6.9. תיעוד

6.9.1. כלל מסמכי העדכון/טלאי יתויקו כחלק ממדיניות ניהול השינויים.

7.השיטה

7.1. תחנות עבודה, שרתים, רכיבי התקשורת, יישומים ומערכות האבטחה הלוגיות בבעלות ממשל זמין יעודכנו בטלאי האבטחה/קושחות העדכניים ביותר) על-מנת להגן על נכסי המידע מפגיעויות ידועות. בנוסף, העדכון יכלול את כלל המחשבים הניידים, מחשבים נייחים והשרתים שבבעלות ממשל זמין או מנוהלים על ידו.

7.2. כלל העדכונים יותקנו על-פי רמת דחיפותם, ראה נספח א' - מועד התקנת עדכונים על-פי דחיפותם (בימים).

7.3. **תחנות עבודה**

7.3.1. מחשבים נייחים ומחשבים ניידים יוגדרו לקבלת עדכונים אוטומטיים לצורך קבלת טלאי האבטחה למערכות ההפעלה. תצורה זו תוגדר כברירת מחדל בכלל תחנות העבודה בממשל זמין.

7.3.2. עדכון יישומים מאושרים המותקנים על תחנת העבודה יתבצעו באמצעות התקנה ידנית או אוטומטית.

7.3.3. עדכון קושחות (BIOS) יתבצע באמצעות כלים ידניים או אוטומטיים.

7.3.4. כל חריגה מהמדיניות הנ"ל תאושר על-ידי מנהל מערך סייבר ואבטחת מידע ותתועד בהתאם.

7.4. **שרתים**

7.4.1. שרתים חייבים לעמוד בדרישות הבסיסיות המינימליות שאושרו ע"י מנהל מערך סייבר ואבטחת מידע.

7.4.2. דרישות בסיסיות מינימליות אלו יגדירו את רמת ברירת המחדל של מערכת ההפעלה, חבילת שירות (Service Pack), HotFix וטלאי האבטחה על-מנת להבטיח את אבטחת נכסי המידע ונתוני המערכת.

7.4.3. עדכון יישומים מאושרים המותקנים על תחנת העבודה יתבצעו באמצעות התקנה ידנית או אוטומטית.

7.4.4. עדכון קושחות יתבצע באמצעות כלים ידניים או אוטומטיים.

7.4.5. כל חריגה מהמדיניות הנ"ל תאושר על-ידי מנהל מערך סייבר ואבטחת מידע ותתועד בהתאם.

7.5. **רכיבי תקשורת**

7.5.1. רכיבי התקשורת (LoadBalancer ,Switch ,Router) יעודכנו מעת לעת על-פי ספק המוצר הרלוונטי.

7.5.2. עדכון קושחות יתבצע באמצעות כלים ידניים או אוטומטיים.

7.5.3. כל חריגה מהמדיניות הנ"ל תאושר על-ידי מנהל מערך סייבר ואבטחת מידע ותתועד בהתאם.

7.6. **מערכות האבטחה הלוגיות**

7.6.1. כלל מערכות האבטחה הלוגיות (IPS, IDS, FW, AntiDdos, AV, WAF) יעודכנו מעת לעת על-פי ספק המוצר הרלוונטי.

7.6.2. כל חריגה מהמדיניות הנ"ל תאושר על-ידי מנהל מערך סייבר ואבטחת מידע ותתועד בהתאם.

7.7. **בדיקות**

7.7.1. צעד חיוני בניהול התקנת טלאי האבטחה הינו להבטיח שהטלאי/קושחה החדש/ה אינו מתנגש עם הסביבה הנוכחית. לצורך כך תבוצע בדיקה לטלאי האבטחה/קושחה בסביבת בדיקות (אם מתאפשר הדבר) טרם התקנתם בסביבת הייצור.

8. ניטור ודיווח

8.1. האחראים ליישום המדיניות הנזכרים בסעיף 4 לעיל נדרשים לאסוף ולשמור את המדדים המדווחים שמסכמים את התוצאות של כל מחזור התקנת טלאי האבטחה/קושחות.

8.2. דוחות אלה ישמשו להערכת רמת הטלאים/קושחות שהותקנה בכל המערכות ועל מנת להעריך את הרמה הנוכחית של סיכון. דוחות אלה יהיו זמינים למערך סייבר ואבטחת מידע ולביקורת שונות על פי דרישה.

9. אכיפה

9.1. יישום ואכיפה של מדיניות זו הינה באחריותם של כלל עובדי ממשל זמין. מערך סייבר ואבטחת המידע וביקורת פנימית עשויים לבצע הערכות אקראיות כדי להבטיח התאמה למדיניות ללא הודעה מוקדמת.

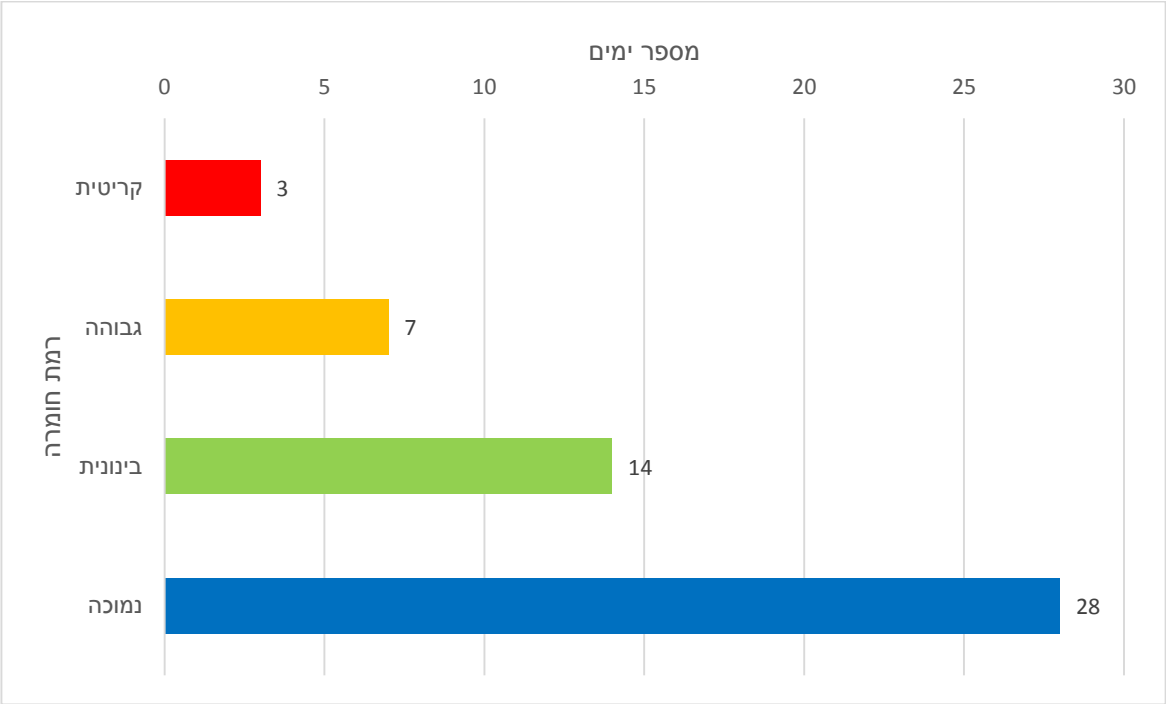
9.2. כל מערכת הנמצאת בהפרה של מדיניות זו תחייב פעולה מידית לתיקון. הפרות תצוינה במערכת המעקב של ממשל זמין וצוותי תמיכה יישלחו לתיקון הנושא.

10. חריגה מהמדיניות

10.1. חריגה מדיניות עדכון טלאי האבטחה/קושחות תדרוש אישור מתועד רשמי ממנהל מערך סייבר ואבטחת מידע. כל השרתים או תחנות העבודה שאינם עומדים במדיניות חייבים להיות מגובים באישור חריג כתוב.

10.2. **כל הנחייה הניתנת על ידי מערך סייבר ואבטחת המידע להתקנת עדכונים קריטיים קודמת להוראות מדיניות זו וגוברת עליהן.**

11. נספח א' - מועד התקנת עדכונים על-פי דחיפותם (בימים)



*- קריטית – על פי הגדרת מערך הסייבר ואבטחת המידע (לא הגדרת יצרן).