נוהל אבטחת תשתיות

משרד הבריאות

ישראל

משרד הבריאות

משרד הבריאות

נוהל אבטחת תשתיות

03/06/2012	חברת אבנת	1.1	כתיבת הנוהל
20/08/2012	תמיר פלדמן	1.2	התאמה לתקן ISO 27799
30/09/2012	שי אמיר	1.3	אישור הנוהל

משרד הבריאות

נוהל אבטחת תשתיות

1. רקע

1.1. במסגרת הנחיות אבטחת מידע למערך הבריאות, נדרשים הנחיות לאבטחת תשתיות המערך.

2. מטרה

2.1. מסמך זה מספק הנחיות אבטחת מידע בתשתיות מערך הבריאות.

3. שיטה

3.1. ניתוח הנחות היסוד.

3.2. ניסוח סיכוני אבטחת המידע.

3.3. הגדרת הנחיות אבטחת המידע בהיבטי תשתיות.

3.4. הגדרת הנחיות כלליות לחסימה של אתרים וקבצים פוגעניים מרשת האינטרנט (מוצג **בנספח א'**).

4. הנחות יסוד

5. סיכוני אבטחת מידע

6. הנחיות אבטחת מידע לתשתיות במערך:

6.1. ניהול רכיבי התקשורת ואבטחת המידע

6.1.1. נדרש לנהל את כלל רכיבי התקשורת ואבטחת המידע באמצעות פרוטוקולים מוצפנים בלבד.

6.1.2. יבוטלו פרוטוקולי ניהול שאינם נדרשים בכלל רכיבי התקשורת ואבטחת המידע.

6.1.3. ממשקי הניהול של כלל הרכיבים ושרתי הניהול השונים יוגדרו עם מדיניות הצפנה ואמינות יחידה (אלגוריתמי ההצפנה ואמינות המידע) ללא יכולת התדיינות עם הרכיב הניגש.

6.1.4. כלל ממשקי הניהול של הרכיבים ושרתי הניהול יבוקרו תקשורתית. נדרשת הגדרת בקרת גישה תקשורתית פרטני (ACL) לכל ממשקי הניהול, לרבות כתובות IP מורשות ושירותים מורשים.

6.1.5. גישה תקשורתית לניהול כלל הרכיבים תאופשר רק לאחר הצלחת תהליך הזדהות.

6.1.6. כלל סיסמאות ברירת המחדל בכלל הרכיבים יוחלפו לסיסמאות בהתאם למדיניות הסיסמאות שתוגדר (נספח).

6.1.7. נדרש ליישם הזדהות מנהלי ציוד התקשורת ומנהלי מערכות הניהול ה/שונות דרך שרת הזדהות מרכזי.

6.1.8. נדרש לנהל את כלל ציוד התקשורת ואבטחת המידע באמצעות מערכות ניהול מרכזיות וייעודיות, בהתאמה.

6.1.8.1. תיושם בקרת גישה תקשורתית למערכות ניהול אלו.

6.1.8.2. הגישה למערכות ניהול אלו תאופשר מעמדות ניהול מאושרות בלבד.

6.1.8.3. נדרש להטמיע את המערכות תוך כדי התאמה לדרישות הזמינות.

6.1.8.4. המערכות ישמשו, בין היתר, עבור ניהול גרסאות מערכת הפעלה / קושחה / חומרה, ניהול הגדרות רכיבים, ניטור מצב הציוד.

6.1.9. נדרש להפעיל בכלל מערכות הניהול מנגנון ניתוק אוטומטי לאחר Timeout ללא פעילות.

6.1.10. ההרשאות הרלוונטיות לפעולות ברכיבים ובשרתי הניהול השונים יוגדרו בהתאם לעיקרון Least-Privileges.

6.1.11. נדרש כי תתבצע הצפנת סיסמאות ומפתחות בקובץ התצורה שברכיבים השונים ללא יכולת שחזור מהטקסט.

6.1.12. נדרשת שליחת חיוויים מהרכיבים לשרת ניטור מרכזי. החיוויים יכילו לפחות את זמן הפעולה, מהות הפעולה ושם המשתמש שביצע את הפעולה. המידע האגור ישמר לפחות למשך חודש.

6.2. קישוריות

6.2.1. נדרש להקשיח את כלל רכיבי התקשורת ברמות 2 ו 3. בין השאר, יש לטפל בנושאים הבאים:

6.2.1.1. יבוטלו כלל השירותים שאינם נדרשים בכל רכיבי התקשורת.

6.2.1.2. נדרש להגדיר בכל מתג את ה – VLANs הנדרשים בלבד. הניתוב בין ה – VLANs לא יבוצע במתגי ה – Access. בקישורי ה – Trunk יוגדרו VLANs נדרשים בלבד.

6.2.1.3. נדרש ליישם מנגנונים לבקרת גישה תקשורתית לרשת. להלן אמצעים רלוונטיים:

6.2.1.3.1. סגירה של פורטים שאינם בשימוש.

6.2.1.3.2. יישום של Port Security, MAC Address Limiting.

6.2.1.3.3. יישום של מנגנוני IEEE 802.1x.

6.2.1.3.4. יישום של רכיב Network Access Control אשר יבצע את התהליכים הבאים:

6.2.1.3.4.1. זיהוי של רכיבים ברשת (בדיקת IP, MAC, שייכות ל – Domain ועוד).

6.2.1.3.4.2. בחינה של אמינות הרכיבים ברשת (למשל בדיקת אנטיוירוס).

6.2.1.3.4.3. אכיפה של מדיניות גישה לרשת.

6.2.1.3.4.4. טיפול ברכיבים השייכים לרשת אך לא עומדים בדרישות האמינות ברשת.

6.2.1.4. נדרשת ליישם מסננים (Access Lists) בשכבת הניתוב, לרבות כתובות מקור ויעד מורשות ושירותים מורשים, בהתאם לצרכים בלבד.

6.3. שירותי התקשורת

6.3.1. נדרש ליישם שירות תזמון Network Time Protocol (NTP) יחד עם תהליך NTP Authentication.

6.3.2. נדרש ליישם שירותי ניתוב דינמי יחד עם תהליך הזדהות ואמינות מידע בין רכיבי הניתוב.

6.3.3. בכלל הרשת יוקצו כתובות IP בהתאם ל – RFC 1918 בלבד.

6.4. שירותי אבטחת המידע

6.4.1. הטמעה של Firewall מרכזי ברשת עם יכולות שרידות. קישוריות רגליו של ה – Firewall למתג מרכזי עם הגדרות 802.1q. ב – Firewall יוגדרו חוקי תעבורה בהתאם לעיקרון ה – Least-Privileges. כלומר: אפשור רק לגורמים נדרשים, גישה לשירותים / רכיבים / שרתים הנדרשים להם, בפרוטוקולים הנדרשים להם, בלבד.

6.4.2. בסגמנטים המכילים מערכות רגישות, בעיקר מערכות החשופות לרשת האינטרנט, מעבר לבקרה על ידי ה – Firewall יקושר גם רכיב Intrusion Prevention (IPS) אשר יגן מפני ניסיונות תקיפה מרשת האינטרנט וניסיונות תקיפה מתגלגלת מתוך סביבות DMZ. <u>רכיב זה יבצע את הדברים הבאים:</u>

6.4.2.1. זיהוי וחסימה של תקיפות DoS ו – DDoS.

6.4.2.2. זיהוי וניטור של ניסיונות איסוף מודיעין עסקי (Host Scan ,Port Scan).

6.4.2.3. זיהוי וחסימה של ניסיונות ניצול חשיפות ותקיפות על מערכות הפעלה, אפליקציות, רכיבי תקשורת ואבטחת מידע (Exploits).

6.4.2.4. זיהוי וחסימה של פעילות בפרוטוקולים מורשים, אך שלא לפי ה – RFC שלהם.

6.4.2.4.1. שמירת לוגים ויצירת התראות בזמן אמת.

6.4.3. יישום של סגמנטציה של שירותים שונים ברשת דרך ה – Firewall באמצעות הפרדה ל - VLANs. <u>בין היתר, תיושם הפרדה של השירותים הבאים:</u>

6.4.3.1. שירותי ניהול של שרתים ושל ציוד תקשורת ואבטחת מידע (לדוגמא: CiscoWorks, NSM, SMS).

6.4.3.2. שירותי אבטחת מידע, כגון: שרתי עדכון של Patches (לדוגמא: WSUS, SMS), שרתי אנטי וירוס מרכזיים, מערכת מרכזית להקשחת שרתים.

6.4.3.3. שירותי הגנה על האפליקציות השונות (WAF) החשופות לרשת האינטרנט. <u>רכיב זה יתמוך בנושאים הבאים:</u>

6.4.3.3.1. הצפנת תווך מול המשתמש - Reverse SSL Proxy.

6.4.3.3.2. יצירת ועדכון פרופילים דינמיים של אפליקציות ושל משתמשים (מי ניגש, מאיזה URL ולאן, פעולות מותרות ועוד).

6.4.3.3.3. זיהוי חתימות של התקפות ידועות במספר רבדים (מערכת הפעלה, אפליקציה,SQL Injection, Known worms, OS Vulnerabilities, Zero-days Worms, DoS Attacks).

6.4.3.3.4. Protocol RFC Compliance (HTTP/S, SQL ועוד).

6.4.3.3.5. שליטה דינמית ב - Session, הגדרת החלטות לביצוע לפי כל ישות בשכבה 7.

6.4.3.3.6. מיסוך של מידע (שרתי WEB, הודעות שגיאה של אפליקציות או אתרים, מידע רגיש, כגון מספרי אשראי, זהות).

6.4.3.3.7. מנגנוני הקשחה (Cookie Signing and Encryption, URL Rewriting, בקרת גישה לאתרים ברמת כתובת בקשת HTTP, URL, תוכן, Cookies.

6.4.3.3.8. שילוב של הגנה על ה – Database ומעקב אחרי גישת משתמשים למידע.

6.4.4. שירותי גישה מרחוק מאובטחת עבור ספקים. להלן פירוט תהליכי הגישה המאובטחת (Security Policy) בהתאם לסדר הדרוש:

6.4.4.1. הספק יפנה לאתר ה – SSL-VPN בשירות SSL מוצפן.

6.4.4.2. תבוצע סריקת התקני קצה Host/Health Checker, מטרתה של יישום זה היא לסרוק תחנה מרוחקת בזמן שזו מנסה לגשת באמצעות VPN למשאבי הארגון. הסריקה של Host Checker תוגדר עבור הדברים הבאים: קיום תוכנת אנטי וירוס פעילה ודרסת החתימות שלה, קיום Personal Firewall.

6.4.5. הספק יבצע הזדהות עם אמצעי הזדהות חזקה, לדוגמא: Token ו\או רכיב OTP על מנת לצמצם ככל האפשר את סיכוי של התחזות. תהליך ההזדהות וקבלת ההרשאות הרלוונטיות ייושם דרך שרת Active Directory.

6.4.6. תיושם גישה מה – SSL-VPN לשרת ה-Terminal אשר יספק ממשק אפליקטיבי למתחברים מרחוק. גם בשרת זה תבוצע הזדהות מול ה – Active Directory.

6.4.7. בשרת ה – Terminal יותקנו האפליקציות הנדרשות, ויוגדרו ההרשאות הרלוונטיות לספקים השונים, בהתאם לצרכי התחזוקה. ב – Firewall יוגדרו חוקי תעבורה מכיוון ה – Terminal לכיוון השרתים הרלוונטיים, המתוחזקים על ידי ספק חיצוני. יש להדגיש שתעבורה מול המערכות השונות תאופשר ה – Terminal בלבד.

6.4.8. על מנת לצמצם את הסיכון של תקיפה מתגלגלת, משרת אחד של מערכת מנוהלת על ידי ספק חיצוני לשרת אחר, שאינו נדרש לתחזוקה של ספק חיצוני, נדרש להפריד את השרתים הרלוונטיים לסגמנט יעודי (אחד או יותר) ולצמצם עד כמה שניתן את ההרשאות הניתנות לספקים השונים בשרתים הרלוונטיים.

6.4.9. נדרש ניטור של כלל התעבורה העוברת ברכיבים מרכזיים ברשת. הלוגים יועברו למערכת SIM שמטרתה לזהות ולמנוע ניסיונות לביצוע הונאות, פגיעה בשירותים, חשיפת / שינוי מידע רגיש.

6.4.10. כלל ה – Firewalls ברשתות יוטמעו בהתאם לכללים הבאים:

6.4.10.1. הגישה ל – WAN ומה – WAN, למערכות משיקות / חיצוניות וממערכות משיקות / חיצוניות תבוקר תקשורתית על ידי ה - Firewall.

6.4.10.2. הגדרת Statefull Inspection.

6.4.10.3. תצורת Cluster.

6.4.10.4. סגירת שירותים שאינם נדרשים.

6.4.10.5. הגדרה של ממשקי תקשורת בהתאם לדרישות הפונקציונאליות בלבד.

6.4.10.6. הגדרה של מדיניות גלובלית בצורה שתצמצם את הפגיעה בזמינות, אמינות וחשאיות הרכיב והסביבות שעליהן הוא מגן.

6.4.10.7. הגדרה של מדיניות בקרת גישה תקשורתית ברכיב בהתאם לדרישות הפונקציונאליות בלבד יחד עם צמצום סיכוני הפגיעה בזמינות, חשאיות ואמינות המידע ברכיב ובסביבות / מערכות שעליהן הוא מגן.

6.4.10.8. יוגדרו הגדרות בחינת וסינון תכנים פוגעניים ברובדי תקשורת 2-7.

6.4.11. עבור גלישה ברשת האינטרנט יוטמע שרת Proxy בסביבת DMZ. שרת זה יבצע את הדברים הבאים:

6.4.11.1. Forward Proxy לגלישה באינטרנט, עם כתובת אינטרנט של המוגדרת ומנוהלת על ידי ה – ISP.

6.4.11.2. בדיקת וירוסים.

6.4.11.3. בקרת קבצים הנכנסים / יוצאים מהרשת לרשת האינטרנט (באמצעות זיהוי Mime Type). הסברים מופיעים **בנספח א'.**

6.4.11.4. בקרת גישה לאתרים באינטרנט (URL Filtering). הסברים מופיעים **בנספח א'.**

6.4.11.5. אפשור גישה לאתרים באינטרנט לגורמים ברשת בהתאם למדיניות המוגדרת לפי שם המשתמש (לאחר הזדהות), כתובת ה – IP, הרשאות המתאימות.

6.4.11.6. בדיקת פעילות של פרוטוקולי אינטרנט בהתאם לסטנדרט הבינלאומי הרלוונטי (כדוגמת HTTP RFC).

6.4.11.7. הטמעה של הזדהות משתמשים.

6.4.11.8. נדרש לשמור לוגים לפי מדיניות מוגדרת ושליחת Alerts בזמן אמת למנהלי המערכת.

6.4.11.9. נדרש להגדיר זיהוי וחסימה של Spywares / Malwares באמצעות השיטות הבאות:

6.4.11.9.1. חסימת Exploits ידועים, בהתאם לחתימות.

6.4.11.9.2. ביצוע Striping של Executable Downloads מאתרים מורשים.

6.4.11.9.3. ביצוע חיפוש היוריסטי אחר וירוסים וסוסים טרויאניים באמצעות תוכנת Anti-Virus תקנית ועדכנית.

6.4.11.10. חסימה אוטומטית של אתרי Phishing ידועים.

6.4.11.11. מניעת משתמשים להעביר מידע לאתרים בעלי סיכון גבוה (למשל אתרים עם סרטיפיקט לא מעודכן).

6.4.11.12. יישום עבודה כ – SSL Proxy באופן מלא. כלומר הגדרת ניטור של תעבורה מוצפנת (HTTPS/SSL).

6.4.11.13. הגדרת ניטור ובקרה של תעבורות Streaming Video / Audio.

6.4.11.14. זיהוי וניטור של תעבורת IM (Native & HTTP) באמצעות הגדרת White-List. יישום של מדיניות File-Transferring Blocking ,File-Type/Key-Words Filtering באפליקציות IM בשני הכיוונים (עמ"נ למנוע פגיעה ברשת ע"י וירוסים).

6.4.11.15. זיהוי, ניטור וחסימה של אפליקציות P2P.

6.4.12. יוטמע שרת Audit מרכזי אשר יאסוף מידע מכלל השרתים, המערכות ומערכות הניהול של כלל הרכיבים, יבצע קורלציה בין אירועים, יציג את אירועי אבטחת המידע בזמן אמת, יאפשר תחקור של אירועים היסטוריים ויציג דוחות רלוונטיים לגורמי אבטחת המידע.

נספח א' - עקרונות בסיסיים לחסימה של אתרים וקבצים בערוצי האינטרנט

1. כיום קיימים סיכוני אבטחת מידע רבים בגלישה לאתרי אינטרנט שונים ובקבלה של קבצים דרך שירותי אינטראנט. סיכונים אלו מאיימים על אמינות ושלמות המידע וכן על זמינות המידע והתשתיות ברשת. נספח זה מספק את העקרונות הבסיסיים לחסימה של אתרים ושל קבצים בערוצי האינטרנט.

2. **Instant Messaging (IM) -** לא מומלץ לאפשר עבודה עם אפליקציות IM דרך האינטרנט. ה – IM דורש קישוריות בין תחנות קצה בתוך הרשת לשרתים / תחנות קצה מחוץ לרשת, דרך רשת האינטרנט ושירותים החשופים לפגיעויות כמו HTTP ו – SOCKS. תוקף פוטנציאלי יכול להחדיר קודים זדוניים לתחנות הקצה ולרשת, לאחר התחזות פשוטה. אפליקציות ה – IM מאפשרות שיתוף תיקיות וקבצים ולכן מאפשרות חשיפה של מידע רב מתוך הרשת לגורמים חיצוניים לא מורשים.

3. **Peer-to-Peer (P2P) -** נדרש לחסום כל שימוש ב - Peer-to-Peer ברשת דרך האינטרנט. נדרש לחסום ולתעד כל ניסיון ליצירת קישור P2P מול האינטרנט. קיימים הסיכונים הבאים בשימוש ב – P2P:
   3.1. ניצול של רוחב סרט גדול ברשת עלול לפגוע במערכות קריטיות ברשת.
   3.2. סיכון גבוה של חשיפה לוירוסים וקודים זדוניים שונים ממקורות באינטרנט.
   3.3. סיכונים של עבירה על החוק בעת הורדה של קבצי מוסיקה וסרטים המוגנים על ידי זכויות יוצרים.

4. **מהם הנושאים הרלוונטיים בחסימה של אתרים באינטרנט ?**
   4.1. <u>בחינת מיקום והגורם המנהל את האתר:</u> אם מנהל האתר הוא גוף קטן יחסית, אדם בודד, גורם עברייני, גורם עוין, לא אמין, אינו מוגדר או אינו ידוע או קיים מידע סותר לגביו ברשומות ה – DNS

(כמו אתרי רדיו וטלוויזיה, אתרי קניות, אתרי חדשות, אתרים לא חוקיים, אתרי עירום, אתרי אלימות ועוד), קיים סיכון שרמת אבטחת האתר נמוכה, מה שמאפשר ניצול לרעה של האתר מול רשתות ארגונים.

4.2. בחינת סיכונים כלליים של האתר: מידע עדכני לגבי חולשות שנוצלו – סיכון לניצול של חולשות מול מחשבים או מול תוכנות רלוונטיות ברשת (למשל אתרי רשת חברתית כמו Facebook, ניצול חולשות ב – Windows Media Player).

4.3. בחינת הפופולאריות של האתר: ככל שהאתר יותר פופולארי בעולם / בארץ (אתרי משחקים, פרסומות, רשתות חברתיות, אתרי רדיו וטלוויזיה, אתרי הורדות קבצים ועוד), כך יותר משתמשים ניגשים אליו, והסיכוי להצלחה של חדירות או פגיעות באבטחת המידע, גבוה יותר עבור תוקף פוטנציאלי. לכן, תוקפים יעדיפו להשתמש באתרים פופולאריים על מנת לנסות ולנצל חולשות שונות בתחנות קצה רבות ובארגונים רבים (שם קיים סיכוי להצלחה, בגלל כמות הארגונים), מאשר אתרים שאינם פופולאריים. לפיכך, השימוש באתרים פופולאריים מגדיל את סיכוני אבטחת המידע ברשת הארגונית.

4.4. בחינת מהות האתר:

4.4.1. אתרים המאפשרים הורדה / העלאה של קבצים ושיתוף מידע

(לדוגמא: אתרי רשתות חברתיות, אתרי משחקים, אתרי Utilities, אתרי שיתוף מוסיקה וסרטים) מגדילים את סיכון אבטחת המידע לרשת, מכיוון שהם מאפשרים להעביר קבצים זדוניים לתחנות הקצה ומהווים מוקד לתוקפים בעלי מוטיבציה גבוהה, המנצלים את הפופולאריות על מנת ליצור: Exploits, תקיפות ממוקדות, אתרים מתחזים.

4.4.2. אתרים הפועלים בתצורת Stream (אתרי רדיו וטלוויזיה):

4.4.2.1. מדובר באתרים פופולאריים, המנוהלים על ידי גופים לא גדולים שאינם מחשיבים את אבטחת אתרם כיעד מרכזי בשירות שהם מספקים. לכן, אתרים אלו חשופים לפגיעויות מצד גורמים עוינים.

4.4.2.2. בדרך כלל מבוצע שימוש בתוכנות ייעודיות בתחנת הקצה (RealAudio, Windows Media Player, Winamp) המכילות חשיפות שניתן לנצלן על ידי Exploits הידועים באינטרנט.

4.4.2.3. הפעילות מול אתרי ה – Streaming היא בדרך כלל ב – Unicast. כל משתמש פונה ומקבל ערוץ ישיר ואישי של רדיו. אם שישור לכל משתמש צורך כ – 300Kbps, עבור 500 משתמשים בו-זמנית מדובר בכ – 15Mbps. רוחב סרט גבוה יחסית זה יכול להשבית את שירותי התקשורת החיצוניים.

4.4.3. אתרי רשתות חברתיות: מאפשרים הוספה / הורדה של קבצים, שיתוף מידע ועוד. קיימת מוטיבציה של תוקפים בכל העולם לנצל חולשות שונות בתחנות הקצה הניגשות לאתרים חברתיים (בגלל הפופולאריות) על מנת לגנוב מידע או לשבש מידע ארגוני. באתר זה יכול להתפרסם מידע

אישי רב על ידי המשתמשים, כאשר הבקרה על התכנים והשימוש בהם ניתן למשתמש בלבד, ללא יכולת של בקרה דיגיטלית מרכזית על ידי רכיב ה – BlueCoat, על מהות המידע או על דרכי השימוש בו באתר. אתר זה משמש קרקע לגורמים עוינים למציאה ושימוש במידע אישי של משתמשים לביצוע גניבות פיננסיות ואף לגניבת זהות מלאה.

4.4.4. אתרי שיתוף סרטים ומוסיקה (Media) – אתרים המאפשרים הורדה של קבצים, אשר חלקם עלולים להיות גם קבצים זדוניים שנועדו לאפשר השתלטות על תחנות קצה.

4.4.5. שרתי Anonymous Proxies – שרתים המאפשרים התקשרות מולם ב – SSL ומהווים מתווך תקשורתי מול אתרי האינטרנט. הקישור המוצפן מאפשר לגורם פנימי עוין לעקוף את כלל מנגנוני הבקרה הקיימים ברשת על מנת להעביר קבצים זדוניים לרשת.

5. מהם הסיכונים העיקריים מקבצים מהאינטרנט ?

5.1. קבצי Executable – קבצים אשר מורצים על ידי מערכת ההפעלה (EXE ,COM, BAT) שבתחנת הקצה או על ידי תוכנות מותקנות כגון Office, Acrobat Reader, MS-DOS. קבצים אלו מאוד מסוכנים מכיוון שדרכם ניתן להחדיר קודים זדוניים שבהפעלתם הם פוגמים בתחנת העבודה ומתפשטים לתחנות עבודה אחרות.

5.2. קבצים היכולים להכיל / מכילים Macros (Office, MDB) – יכולים לפגוע רק אם מופעלים על ידי האפליקציות הרלוונטיות. יכולים להריץ קודים זדוניים המוחבאים בתוכם.

5.3. קבצי קישורים, הפניות (lnk, pif, url) – יכולים להפנות למיקומים לא צפויים בהפעלתם. לכן מהווים סיכון מסוים ברשת ארגונית.

5.4. קבצים אשר ניתן להסתיר בהם Exploits מסוגים שונים מול חולשות קיימות בתחנות הקצה– בסוגי קבצים אלו קיים סיכון מעצם תדירות ה – Exploits שבהם (אפליקציות חשופות לדוגמא: Windows Media Player, Office, internet Explorer, Acrobat Reader).