

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 1 מתוך 12	א.1.13	

ניהול אישורים

<u>תאריך</u>	<u>שם</u>	<u>תפקיד</u>	<u>חתימה</u>
30/09/2012	שי אמיר	ממונה אבטחת מידע	שי
01/03/2016	שי אמיר	ממונה אבטחת מידע	שי
01/08/18	ראובן אליהו	ממונה אבטחת מידע	ראובן

ניהול שינויים

<u>תאריך</u>	<u>מחבר</u>	<u>גרסא</u>	<u>מהות השינוי</u>
03/06/2012	חברת אבנת	1.1	כתיבת הנוהל
20/08/2012	תמיר פלדמן	1.2	התאמה לתקן ISO 27799
01/03/2016	גבי פטליס	1.4	עדכון על פי דרישות תקן גרסה 2013: עדכון מספר נוהל תיקון שם נוהל על פי התקן
01/01/2018	אורנסק	1.5	התאמה ל- iso 27799:2016

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 2 מתוך 12	א.13.1	

1. מטרה

1.1 מסמך זה מספק הנחיות אבטחת מידע בתשתיות משרד הבריאות.

2. הגדרות

2.1 אמ"ל.

3. מסמכים ישימים

3.1 אמ"ל.

4. אחריות ליישום

4.1 מנהל מערכות מידע.

5. שיטה

5.1 מערכות המידע במשרד הבריאות משמשות לאחסון ועיבוד מידע רגיש, החיוני להמשך פעילותו התקיין של משרד הבריאות.

5.1 שימוש בלתי נאות במערכות המידע, בזדון או בשוגג, עלול לחשוף את משרד הבריאות בפני סיכוני אבטחה ולהוביל לפגיעה בהיבטים התפעוליים, העסקיים והתדמיתיים של משרד הבריאות.

5.2 בקרה הולמת אחר הפעילויות המבוצעות במערכות המידע, תוכל להביא לאיתורן של פעולות חריגות, כגון ניסיונות חדירה בלתי מורשית למערכות, ניסיונות לשיבוש או מחיקה בלתי מורשים של מידע, פגיעה ברכיבי המערכות וכיוצא באלו.

5.3 ניהול רכיבי התקשורת ואבטחת המידע :

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

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

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

5.3.4 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.

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 3 מתוך 12	א.13.1	

- 5.3.5 הגישה לממשקי ניהול של ציוד תקשורת ואבטחה תנוטר.
- 5.3.6 גישה תקשורתית לניהול כלל הרכיבים תאופשר רק לאחר הצלחת תהליך הזדהות ועפ"י פרופיל הרשאות.
- 5.3.7 כלל סיסמאות ברירת המחדל בכלל הרכיבים יוחלפו לסיסמאות בהתאם למדיניות הסיסמאות שתוגדר.
- 5.3.8 נדרש לנהל את כלל ציוד התקשורת ואבטחת המידע באמצעות מערכות ניהול מרכזיות וייעודיות, בהתאמה.
- 5.3.9 תיושם בקרת גישה תקשורתית לממשקי הניהול.
- 5.3.10 הגישה למערכות ניהול אלו תאופשר מעמדות ניהול מאושרות בלבד.
- 5.3.11 נדרש להטמיע את המערכות תוך כדי התאמה לדרישות הזמינות.
- 5.3.12 תיושם מערכת ניהול תשתיות. בין היתר תשמש עבור ניהול גרסאות מערכת הפעלה / קשוחה / חומרה, ניהול הגדרות רכיבים, ניטור מצב הציוד.
- 5.3.13 נדרש להפעיל בכלל מערכות הניהול מנגנון ניתוק אוטומטי מקוצר לאחר אי שימוש.
- 5.3.14 ההרשאות הרלוונטיות לפעולות ברכיבים ובשרתי הניהול השונים יוגדרו בהתאם לעיקרון Least-Privileges.
- 5.3.15 נדרש כי תתבצע הצפנת סיסמאות ומפתחות בקובץ התצורה שברכיבים השונים ללא יכולת שחזור מהטקסט.
- 5.3.16 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 24 חודש.
- 5.4 קישוריות :
- 5.4.1 נדרש להקשיח את כלל רכיבי התקשורת ברמות נתבים ומתגים. בין השאר, יש לטפל בנושאים הבאים :
- 5.4.1.1 יבוטלו כלל השירותים שאינם נדרשים בכל רכיבי התקשורת.
- 5.4.1.2 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.

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 4 מתוך 12	א.13.1	

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

5.4.2.1. סגירה של פורטים שאינם בשימוש.

5.4.2.2. יישום של Port Security, MAC Address Limiting.

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

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

5.4.2.3.2. בחינה של אמינות הרכיבים ברשת (למשל בדיקת אנטי-וירוס).

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

5.4.2.4. נדרש ליישם רשימת סינון, לרבות כתובות מקור ויעד מורשות ושירותים מורשים, בהתאם לצרכים בלבד.

5.5. שירותי התקשורת :

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

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

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

5.6. שירותי אבטחת המידע :

5.6.1. 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 : אפשר רק לגורמים נדרשים, גישה לשירותים / רכיבים / שרתים הנדרשים להם, בפרוטוקולים הנדרשים להם, בלבד.

5.6.2. 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. רכיב זה יבצע את הדברים הבאים :

5.6.2.1. זיהוי וחסימה של תקיפות Do's ו – DDoS.

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

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 5 מתוך 12	א.13.1	

- 5.6.2.3. זיהוי וחסימה של ניסיונות ניצול חשיפות ותקיפות על מערכות הפעלה, אפליקציות, רכיבי תקשורת ואבטחת מידע (Exploits).
- 5.6.2.4. זיהוי וחסימה של פעילות בפרוטוקולים מורשים, אך שלא לפי ה – RFC שלהם.
- 5.6.2.5. שמירת לוגים ויצירת התראות בזמן אמת.
- 5.6.3. יישום של סגמנטציה של שירותים שונים ברשת דרך ה – Firewall באמצעות הפרדה ל - VLANs. בין היתר, תיושם הפרדה של השירותים הבאים:
- 5.6.3.1. שירותי ניהול של שרתים ושל ציוד תקשורת ואבטחת מידע (לדוגמא : Cisco, SMS, NSM).
- 5.6.3.2. שירותי אבטחת מידע, כגון: שרתי עדכון של Patches (לדוגמא : WSUS), שרתי אנטי וירוס מרכזיים, מערכת מרכזית להקשחת שרתים.
- 5.6.4. שירותי הגנה על האפליקציות השונות (WAF) החשופות לרשת האינטרנט, רכיב זה יתמוך בנושאים הבאים:
- 5.6.4.1. הצפנת תווך מול המשתמש - Reverse SSL Proxy.
- 5.6.4.2. יצירת ועדכון פרופילים דינמיים של אפליקציות ושל משתמשים (מי ניגש, מאיזה URL ולאן, פעולות מותרות ועוד).
- 5.6.4.3. זיהוי התקפות ידועות במספר רבדים (מערכת הפעלה, אפליקציה, SQL, DoS Attacks, OS Vulnerabilities Injection, Known worms).
- 5.6.4.4. Protocol RFC Compliance (HTTP/S, SQL ועוד).
- 5.6.4.5. שליטה דינמית ב - Session, הגדרת החלטות לביצוע לפי כל ישות בשכבה 7.
- 5.6.4.6. מיסוך של מידע (שרתי WEB, הודעות שגיאה של אפליקציות או אתרים, מידע רגיש, כגון מספרי אשראי, זהות).
- 5.6.4.7. מנגנוני הקשחה (URL Rewriting, Cookie Signing and Encryption, בקרת גישה לאתרים ברמת כתובת בקשת HTTP, URL, תוכן, Cookies).
- 5.6.4.8. שילוב של הגנה על ה – Database ומעקב אחרי גישת משתמשים למידע.
- 5.6.5. שירותי גישה מרחוק מאובטחת עבור ספקים. להלן פירוט תהליכי הגישה המאובטחת (Security Policy) בהתאם לסדר הדרוש:
- 5.6.5.1. הספק יתחבר לרשת החברה באמצעות שירות VPN SSL.

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 6 מתוך 12	א.13.1	

- 5.6.5.2. תבוצע סריקת התקני קצה Host/Health Checker, מטרתה של יישום זה היא לסרוק תחנה מרוחקת בזמן שזו מנסה לגשת באמצעות VPN למשאבי משרד הבריאות. הסריקה של Host Checker תוגדר עבור הדברים הבאים: קיום תוכנת אנטי וירוס פעילה ודרסת החתימות שלה, קיום Personal Firewall.
- 5.6.5.3. הספק יבצע הזדהות עם אמצעי הזדהות חזקה, לדוגמא: Token וואו רכיב OTP על מנת לצמצם ככל האפשר את סיכוי של התחזות. תהליך ההזדהות וקבלת ההרשאות הרלוונטיות ייושם דרך שרת Active Directory.
- 5.6.6. תיושם גישה מה – SSL-VPN לשרת ה-Terminal אשר יספק ממשק אפליקטיבי למתחברים מרחוק. גם בשרת זה תבוצע הזדהות מול ה – Active Directory.
- 5.6.7. 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, המתחזקים על ידי ספק חיצוני. יש להדגיש שתעבורה מול המערכות השונות תאופשר ה – Terminal בלבד.
- 5.6.8. 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, ככל הניתן, את השרתים הרלוונטיים לסגמנט ייעודי (אחד או יותר) ולצמצם עד כמה שניתן את ההרשאות הניתנות לספקים השונים בשרתים הרלוונטיים.
- 5.6.9. נדרש ניטור של כלל התעבורה העוברת ברכיבים מרכזיים ברשת. הלוגים יועברו למערכת SIEM שמטרתה לזהות ולמנוע ניסיונות לביצוע הונאות, פגיעה בשירותים, חשיפת / שינוי מידע רגיש.
- 5.6.10. כלל ה – Firewalls ברשתות יוטמעו בהתאם לכללים הבאים :
- 5.6.10.1. הגישה ל – WAN ומה – WAN, למערכות משיקות / חיצוניות וממערכות משיקות / חיצוניות תבוקר תקשורתית על ידי ה – Firewall.
- 5.6.10.2. יישום State full Inspection.
- 5.6.10.3. תצורת Cluster.
- 5.6.10.4. סגירת שירותים שאינם נדרשים.
- 5.6.10.5. הגדרה של ממשקי תקשורת בהתאם לדרישות הפונקציונאליות בלבד.

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 7 מתוך 12	א.13.1	

5.6.10.6 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.

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

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

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

5.6.11.2 בדיקת וירוסים.

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

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

5.6.11.5 אפשר גישה לאתרים באינטרנט לגורמים ברשת בהתאם למדיניות המוגדרת לפי שם המשתמש (לאחר הזדהות), כתובת ה-IP, הרשאות המתאימות.

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

5.6.11.7 הטמעה של הזדהות משתמשים.

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

5.6.11.9 נדרש להגדיר זיהוי וחסמה של Spywares / Malwares באמצעות השיטות הבאות:

5.6.11.9.1 חסימת Exploits ידועים, בהתאם לחתימות.

5.6.11.9.2 ביצוע Striping של Executable Downloads מאתרים מורשים.

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

5.6.11.10 חסימה אוטומטית של אתרי Phishing ידועים.

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 8 מתוך 12	א.13.1	

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

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

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

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

5.6.11.15. זיהוי, ניטור וחסימה של אפליקציות P2P.

5.6.12. 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 ויצג דוחות רלוונטיים לגורמי אבטחת המידע.

5.7. בקרה על רשתות אלחוטיות :

5.7.1. יש לוודא כי התקנים אלחוטיים המחוברים לרשת תואמים את הגדרת המדיניות להתקנים מורשים. התקן מורשה הינו התקן, אשר הוגדרה לו הקונפיגורציה, תועדו בעלי ההתקן והצרכים העסקיים לחיבורו לרשת. על המשרד למנוע גישה להתקנים, אשר אינם עומדים במדיניות זו.

5.7.2. יש לוודא קונפיגורציה נאותה של כלי מיפוי הסיכונים (Vulnerability Scanning) לגלות משדרים אלחוטיים המחוברים אל הרשת הארגונית הקווית. התקנים שזוהו ברשת, צריכים לעבור אישור אוטומטי אל מול רשימה של התקנים אלחוטיים מורשים לחיבור לרשת. התקנים, שאינם מאושרים לחיבור לרשת צריכים להיות מנוטרלים בתגובה מידית.

5.7.3. בכדי ליישם מדיניות זיהוי חדירות אלחוטיות לארגון, ניתן לשקול פתרון לזיהוי תקיפות בווקטור ה-Wireless. פתרון Wireless (Wireless Intrusion Detection and Prevention) WIDPS מזהה מתקפות ברמת הרשת ונסיונות פריצה מוצלחים. כמו כן, כלל התעבורה לכיוון הרשת החוטית, צריכה לעבור סינון ולהיות מנוטרת באופן רציף.

5.7.4. בעת זיהוי צורך עסקי לשימוש ברשת אלחוטית ארגונית, יש להגדיר מדיניות פרטנית על נקודות הקצה המאפשרת חיבור לרשתות ספציפיות המוגדרות במשדרי האלחוט הארגוניים.



1.5	מהדורה
ינואר 2018	בתוקף מ
עמוד 9 מתוך 12	א.13.1

- 5.7.5 בעת חוסר קיום דרישה עסקית לשימוש בציוד אלחוטי, יש לנטרל יכולת זו על גבי ציוד הקצה ולהגן על הגדרות אלו מפני שינוי בצורה הולמת.
- 5.7.6 יש לוודא כי הרשתות האלחוטיות, אשר מפורסמות בארגון יישמו הצפנה חדישה בהתאם לסטנדרטים המקובלים. בעת כתיבת המסמך הסטנדרט המקובל הינו WPA2 עם פרוטוקול הצפנה AES, לכל הפחות.
- 5.7.7 יש לוודא כי הרשתות האלחוטיות הארגוניות משתמשים בפרוטוקול הזדהות כגון: EAP/TLS (Extensible Authentication Protocol-Transport Layer Security), המאפשר הגנה והזדהות הדדית בין הציוד המתחבר לבין הציוד המחובר.
- 5.7.8 יש לוודא כי מופעלת היכולת של AP Isolation - ביטול אופציית תקשורת בין ציוד הקצה עצמו בתצורת Peer-To-Peer, אלא אם קיים צורך ברור להפעלת תכונה זו.
- 5.7.9 יש לבטל תקשורת אלחוטית דרך אמצעים פריפריאליים כגון: תקשורת Bluetooth, תקשורת NFC, תקשורת Ethernet-Over-USB, אלא אם קיימת דרישה עסקית ברורה להפעלת אחת מתכונות אלו.
- 5.7.10 בעת חיבור התקנים, אשר אינם שייכים לארגון (BYOD (Bring-Your-Own-Device), יש להפריד אותם משאר ציוד הרשת האלחוטי. ההפרדה תיעשה על ידי יצירת VLAN (Virtual LAN – רשת מופרדת).
- 5.7.11 הרשת תתקשר עם רשת האינטרנט דרך מנגנוני הסינון המקובלים במשרד.
- 5.7.12 הרשת תתקשר עם המשאבים הפנימיים בעת הצפת מדיניות עסקית ברורה. מדיניות זו תתייחס לרשת הזו כרשת זרה ולא בטוחה (Untrusted Network).
- 5.7.13 רשת זו תנוטר באמצעים ייעודיים ותעבור סינון בהתאם להגדרות המחמירות ביותר.
- 5.7.14 המשרד יישם מדיניות סריקה, גילוי רשתות והגנתן באמצעות כלים מסחריים ייעודיים להגנת רשתות אלחוטיות. בנוסף לכך צוות אבטחת המידע של המשרד יבצע ביקורות תקופתיות על התעבורה העוברת ברשתות האלחוטיות. כמו כן, יבצע הצוות ביקורות אלחוט באמצעות כלים ייעודיים בכדי לבדוק את רמת האבטחה של הרשתות הארגוניות.
- 5.7.15 באם קיימות רשתות ארגוניות בעלות אלגוריתמי הצפנה חלשים, הם מסכנות את הארגון, ולכן יש לזהותן ולחזק את רמת האבטחה שלהן. באם לא ניתן לחזק את מערכות ההגנה שלהן, יש לתת את הדעת על הגנות ובקורות מפצות, אשר ישמרו על חסיון המידע ככל הניתן.
- 5.7.16 הצוות יכלול סריקות אוטומטיות בכדי לזהות רשתות, אשר אינן עומדות בדרישות האבטחה של הארגון. המשרד יישם בקורות אוטומטיות לזיהוי רשתות אלו ואף חסימתן.

		אבטחת תשתיות ISO 27799
1.5	מהדורה	
ינואר 2018	בתוקף מ	
עמוד 10 מתוך 12	א.13.1	

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. בחינת מיקום והגורם המנהל את האתר: 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).



1.5	מהדורה
ינואר 2018	בתוקף מ
עמוד 11 מתוך 12	א.13.1

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 סיכויי 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 שידור לכל משתמש צורך כ- 300Kbps, עבור 500 משתמשים בו-זמנית מדובר בכ- 15Mbps. רוחב סרט גבוה יחסית זה יכול להשבית את שירותי התקשורת החיצוניים.



1.5	מהדורה
ינואר 2018	בתוקף מ
עמוד 12 מתוך 12	א.13.1

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. אתרי Anonymouse Proxies – שרתים המאפשרים התקשרות מולם ב- SSL ומהווים מתווך תקשורת 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 (url, pif, lnk) – 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 לדוגמה: Windows Media Player, Office, internet Explorer, Acrobat Reader).