מדיניות חיבור מאובטח

בין אתרי אינטרנט

ושירותי רשת ממשלתיים

גרסה 1.0

מסמך זה כולל מידע השייך לממשל זמין, רשות התקשוב הממשלתי. כל חשיפה, שימוש או העתקה של מסמך זה או חלקים ממנו – ללא קבלת אישור בכתב ממנהל מערך ההגנה בסייבר בממשל זמין – אסורה בהחלט. מסמך זה מיועד לעובדי ממשל זמין ולקוחותיו

מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1.0	22.7.2018	אופיר יהב	גרסא ראשונה

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	ראש תחום מתודולוגיות הגנה בסייבר	אופיר יהב	22.7.2018	(חתימה)
נבדקה ע"י	ראש תחום בדיקות אפליקציה	יוגב מזרחי	22.7.2018	(חתימה)
אושרה ע"י	מנהל מערך ההגנה בסייבר	אברהם זרוק	22.7.2018	(חתימה)

תוכן עניינים

1. כללי

1.1 ממשל זמין מנגיש אתרי אינטרנט ושירותי רשת אחרים לשימוש הציבור ולרווחתו וזאת באמצעות חיבור מאובטח.

1.2 ההגנה החזקה ביותר הקיימת כיום על פרטיות ושלמות המידע – בתקשורת לרשת האינטרנט – הינה באמצעות פרוטוקול HTTPS.

1.3 מסמך זה מפרט את קווי המדיניות של ממשל זמין חיבור מאובטח בין אתרי אינטרנט ושירותי רשת ממשלתיים.

1.4 מסמך זה נכתב עבור עובדי ממשל זמין ולקוחותיו – משרדי ממשל ויחידות סמך – לקוחות המארחים את מערכותיהם ושירותיהם בתשתיות ממשל זמין.

2. רקע:

2.1 פרוטוקול HTTP - הלא מוצפן - אינו מגן על מידע מפני יירוט או שינוי – דבר אשר חושף את המשתמשים למעקב, ציתות או שינוי המידע המתקבל באמצעות פרוטוקול זה. התחברות באמצעות פרוטוקול HTTP הלא מוצפן עלולה להביא לחשיפת מידע רגיש אודות משתמשי האתרים והשירותים הממשלתיים ולפגיעה בפרטיות המשתמשים. מידע הנשלח באמצעות פרוטוקול HTTP חשוף בפני יירוט ושינוי מכאן הוא פותח אפשרות גם להתחזות. מידע זה עלול לכלול את זהות הדפדפן, תוכן אתר האינטרנט, מילות חיפוש או כל מידע אחר הנשלח על ידי המשתמש.

2.2 במטרה להתמודד עם איום זה, ארגונים מסחריים רבים אימצו כבר את פרוטוקול HTTPS, או יישמו מדיניות של "*HTTPS בלבד*" ("*רק HTTPS*"), וזאת על מנת להגן על המשתמשים באתרי האינטרנט ושירותי הרשת שלהם.

2.3 משתמשי אתרי אינטרנט ושירותי רשת ממשלתיים ראויים לאותה הגנה. חיבור מאובטח השומר על פרטיות הגולשים הופך להיות הבסיס לכל שירותי האינטרנט, והדבר בא לידי ביטוי במדיניות גופי התקינה האינטרנטיים, בדפדפנים הנפוצים ובמגמות בפועל במגזר האינטרנט.

2.4 דפדפנים נפוצים מסמנים אתרים אשר אינם עושים שימוש בפרוטוקול HTTPS כאתרים 'לא בטוחים' (Non-Secure) ובשלב זה מציגים בפני הגולשים אל אתרים אלו הודעה כי האתר 'אינו בטוח' – עם כל המשמעויות התדמיתיות שבהצגת הודעה זו.

2.5 **לאור כל האמור לעיל, על לקוחות ממשל זמין - משרדי הממשלה ויחידות הסמך - לאמץ את שינוי זה ויתרונותיו ולהתחיל כבר עתה בתהליך הסבת כל שירותיהם לשימוש בפרוטוקול HTTPS. השקעה בנושא זה, תיצור תוך זמן קצר תנאים טובים יותר לפרטיות של כל ציבור הגולשים.**

2.6 **כל פעילות המשתמשים בשירותים המתארחים בתשתיות ממשל זמין צריכה להחשב כפרטית ורגישה.**

2.7 יישום של מדיניות '*רק-HTTPS*' (*HTTPS* בלבד) ימנע מצב של חוסר עקביות, בין משרדים ויחידות סמך, בהגדרה מהו תוכן, או פעילות גלישה, הנחשבים רגישים. בכך יווצר תקן פרטיות בין-משרדי חזק יותר. אתרי רשת אשר לא יעברו הסבה ל-HTTPS יחרגו הן מקו הפרטיות והאבטחה בהם עושה שימוש המגזר הפרטי והן מתקני האינטרנט הקיימים והמתגבשים. הדבר עלול להשאיר את משתמשי האתרים

הממשלתיים חשופים לאיומי אבטחת מידע ויפגעו באימון הציבור בשירותי הממשלה. למרות שרוב אתרי הרשת הממשלתיים עושים כיום שימוש ב-HTTPS, לא היו עד כה הנחיות ברורות בנושא. הנחיה ליישום *'HTTPS בלבד'* ויישום הנחיה זו יעניקו לציבור אפשרות גלישה פרטית ובטוחה וימצבו את שירותי האינטרנט הממשלתיים כמובילים בתחום האבטחה ברשת.

3. מה עושה HTTPS

3.1 פרוטוקול HTTPS מבצע זיהוי ואימות של כל חיבור של תחנת קצה אל אתר או שירות רשת ומצפין כמעט את כל המידע הנשלח בין אתר או שירות הרשת ובין המשתמש. המידע המוגן כולל 'עוגיות', פרטי הגולש, כתובות URL, משלוח טפסים ונתוני שאילתות.

3.2 HTTPS מתוכנן כך שימנע קריאה או שינוי מידע זה במהלך העברתו. פרוטוקול HTTPS הינו שילוב בין HTTP ו-TLS (Transport Layer Security). TLS הוא פרוטוקול רשת היוצר חיבור מוצפן בתווך מאומת המוקם ברשת האינטרנט החשופה לכל.

3.3 דפדפנים ושאר העזרים העושים שימוש בפרוטוקול HTTPS מוגדרים לתת אמון במספר גורמים מאשרים – גורמים מאשרים המוסמכים להפיק תעודות דיגיטליות עבור בעלי האתרים. תעודות דיגיטליות אלו מהוות אישור עבור תחנת הקצה לכך שהאתר המארח אותה אישר כבר את בעלותו על האתר (ה-Domain) בפני הגורם היוצר את התעודה הדיגיטלית – עוד בשלב הפקת התעודה. הדבר מונע מפני אתרים זרים להתחזות לאתרים או שירותי רשת ממשלתיים.

4. מה HTTPS לא עושה

4.1 ל-HTTPS יש מספר מגבלות עיקריות. כתובות IP ושמות מתחם (Domain) של היעד אינם מוצפנים בשלב ההעברה. גם תעבורה מוצפנת עלולה לחשוף בעקיפין פרטי מידע מסוימים – כגון זמן הביקור באתר או גודלם של המשאבים הנדרשים או המידע הנשלח.

4.2 מדיניות של '*רק HTTPS*' מבטיחה את שלמות התקשורת בין שתי מערכות אך לא מבטיחה הגנה מלאה על המערכות עצמן. פרוטוקול HTTPS אינו מתוכנן להגן על אתר מפני חדירה או למנוע משירות רשת מלחשוף מידע אודות המשתמש במהלך פעולתו השגרתית של השירות. יתרה על כן, אם בוצעה פריצה אל תחנת הקצה של המשתמש, תחנת הקצה עלולה לעבור שינוי בהגדרות כך שהתקשרות עתידית באמצעות HTTPS תהיה תחת שליטתו של הפורץ. ההגנות שנותן פרוטוקול ה-HTTPS עלולות להיות מוחלשות או מוסרות כליל באמצעות תעודה דיגיטלית זדונית.

5. אתגרים ושיקולים באימוץ HTTPS

5.1 **ביצועי האתר** – הצפנה מוסיפה תקורות של חישוב. תוכנות וחומרות חדשות עשויות לעמוד בתקורות אלו ללא פגיעה משמעותית בזמני התגובה או הביצועים. אתרים העוסקים בהעברת תוכן או תוכנות שרתים התומכות בפרוטוקולי SPDY או HTTPS/2, אשר נדרשים לעבוד ב-HTTPS (כאשר גולשים אליהם באמצעות דפדפנים נפוצים), עשויים לשפר משמעותית את ביצועיהם כתוצאה מהמעבר ל-HTTPS.

5.2 **שם שרת (Server Name Indication)** – סיומת שם השרת בפרוטוקול TLS מאפשרת שימוש יעיל יותר בכתובת ה-IP כאשר השרת מארח מספר שמות מתחם. עם זאת, טכנולוגיה זו אינה נתמכת על ידי תחנות קצה מיושנות. לאור זאת, יש לבחון שוב את ישימות השימוש בטכנולוגיה זו בראיה של שיפור הביצועים והיעילות.

5.3 **תוכן מעורב (Mixed Content)** – בבניית אתרים בהם נעשה שימוש ב-HTTPS יש להבטיח שכל המרכיבים החיצוניים (תמונות, סקריפטים, פונטים, iFrames וכו') נטענים גם הם באמצעות החיבור המאובטח. דפדפנים חדשים עלולים לחסום טעינת מרכיבים הנטענים בדרך לא מאובטחת גם אם ההצבעה אליהם נעשית מתוך אתר מאובטח. בהסבת אתר ישן לעבודה בפרוטוקול חדש זה יתכן ויהיה צורך במאמץ משולב - אוטומטי וידני – לצורך עדכון, החלפה או הסרה של הצבעות אל מרכיבים הנטענים בדרך לא מאובטחת. במקרים מסוימים יהיה זה החלק המורכב ביותר בתהליך ההסבה.

5.4 **שירותים ו-API-ים** – העברת שירותי רשת הנותנים שירות בעיקר לתחנות קצה שאינן דפדפנים, כגון API-ים (העברה מפרוטוקולים ישנים לפרוטוקול HTTPS), עלולה להתגלות כפעולה מורכבת הדורשת ביצוע בשלבים מאחר ולא ניתן להסתמך על כך שכל תחנות הקצה עובדות גם הן בפרוטוקול HTTPS או שיבצעו בהצלחה פעולת Redirect.

5.5 **תכנון המעבר** – פרוטוקולים ותקני רשת משתנים ומשתפרים מעת לעת, ופגיעויות אבטחת מידע עלולות לצוץ ולדרוש טיפול מיידי. אתרים ושירותי רשת נדרשים לפעול באמצעות פרוטוקול HTTPS בדרך שתאפשר עדכון מיידי של תעודות דיגיטליות, פרוטוקולים התומכים בהצפנה (כולל אפשרות Forward Secrecy) ומרכיבי הגדרה

אחרים. לקוחות ממשל זמין נדרשים ליישם גם את המלצות רשות התקשוב הממשלתי ושאר גורמי ההנחיה ולהיות מעודכנים בדרכי היישום המומלצות.

5.6 **אבטחת תעבורה מלאה (Strict Transport Security)**– אתרים ושירותים הנותנים שירות באמצעות HTTPS חייבים לאפשר גם את HSTS (HTTPS Strict Transport Security) – שתפקידו להנחות את הדפדפנים הנפוצים להתחשב בתעבורת HTTPS. הדבר מפחית את מספר ההפניות הבלתי מאובטחות ומגן על המשתמשים מפני התקפות העלולות להעביר את התקשורת לפרוטוקול HTTP החשוף. כאשר HSTS מאופשר, מתחמים (Domains) העושים בו שימוש יכנסו ל-'רשימת מאובטחים' (בה עושים שימוש כל הדפדפנים הנפוצים) וזאת על מנת להבטיח שמדיניות ה-HSTS תיושם בכל מקרה.

5.7 **אבטחת מערכת שמות מתחם - (Domain Name System Security DNSSEC)** – כאשר מסתיים תרגום ה-**DNS**, DNSSEC אינו מבטיח פרטיות או שלמות התעבורה בין תחנת הקצה וכתובת ה-IP. פרוטוקול HTTPS נותן את האבטחה הנוספת הזו.

6. עלות יישום HTTPS

6.1 יישום תקן של 'רק-HTTPS' כרוך בעלויות – שהן פועל יוצא של זמן פיתוח, רכש תעודות ועלויות תחזוקה לאורך שנים. עלויות אלו משתנות בהתאם לגודל ותשתית האתרים שבאחריות כל משרד ויחידת סמך. אי לכך, יש להערך ליישום הנחיה זו גם מבחינת המשאבים הנדרשים ליישומה.

6.2 עם זאת, חובה לזכור כי פגיעה במרכיבי אבטחת המידע של אתרי הממשלה עלולה לגרום לנו פגיעה במוניטין ונזק ממשי למשתמשי האתרים - דבר אשר אינו ניתן להערכה כספית.

6.3 ניתן לקבל ממערך ההגנה בסייבר אשר בממשל זמין מידע טכני נוסף אשר יוכל לצמצם את עלויות יישום ההנחיה.

7. הנחיות

7.1 במטרה לקדם את היישום היעיל והאפקטיבי של מדיניות HTTPS-Only אתרים ושירותי רשת ממשלתיים **חדשים** חייבים לעמוד בהוראות מסמך זה באופן מיידי.

7.2 לגבי אתרים ושירותים **קיימים**: משרדי הממשלה צריכים לתעדף את יישום ההנחיות תוך ניתוח והערכת סיכונים תוך התחשבות במספר פרמטרים: לדוגמא, אתרים דרכם עובר מידע מזוהה, אישי (פרטי) ורגיש, או כאשר תעבורת האתר הינה גבוהה. אתרים כאלו צריכים לקבל עדיפות ביישום הנחיות אלו ולעבור ליישום פרוטוקול HTTPS מוקדם ככל אפשר.

7.3 משרדי הממשלה חייבים להפוך את כל אתרי ושירותי הממשלה לנגישים באמצעות חיבור מאובטח (HTTPS בלבד, עם HSTS) עד סוף השנה (סוף 2018).

7.4 השימוש ב-HTTPS ברשת הפנימית (Intranet) הינו מומלץ אך אינו נדרש באופן חד משמעי.

7.5 האחראים על יישום הוראות מסמך זה מוזמנים לפנות למערך ההגנה בסייבר בממשל זמין לצורך קבלת הנחיות נוספות אשר יסייעו ביישום ההוראות.

7.6 לשאלות בנוגע למסמך זה, ניתן לפנות למנהל מערך ההגנה בסייבר בממשל זמין. בכתובת az@cio.gov.il תוך ציון '*HTTPS בלבד*' בשדה הנושא.