סייבר ישראל
מערך הסייבר הלאומי

איומים מרכזיים בעת עבודה באמצעות פלטפורמות תמיכת משתמשים מרחוק

איומים מרכזיים בעת עבודה באמצעות פלטפורמות תמיכת משתמשים מרחוק

תוכן עניינים

רקע ותקציר מנהלים

מגפת הקורונה הביאה עמה שינויים רבים לשוק העבודה ובכלל, להם יהיו השפעות רחבות וארוכות שנים. אחת התופעות הבולטות הוא מעבר של יותר ויותר ארגונים להעסקת עובדיהם מהבית. לעיתים עובדים אלו נדרשים לסיוע של גורמי התמיכה הארגוניים בעת התמודדות עם תקלה לא צפויה, שאינה מאפשרת את המשך עבודתם.

פלטפורמות השתלטות מרחוק משמשות ארגונים רבים וכן משתמשים פרטיים לשם מתן/קבלה שירותי תמיכת IT. הללו מממשות יכולת שיתוף באמצעות מתן גישה למחשב אחר לשלוט במחשב שלכם. בזכות אפשרויות שיתוף מסך, קבצים ושיחה (audio), התוכנה הופכת את מתן השירות ליעיל יותר ובאפשרות תומך ה-IT לפתור את התקלה מרחוק. ההבדל בין שימוש בפלטפורמות אלו לבין פגישה פיזית רגילה, מתייחס למושגים "זמן" ו"מיקום". בזכות הפלטפורמות, ישנה אפשרות לחסוך את זמן ההגעה, דרך ההגעה וזמן פנוי במהלך השבוע על מנת לתקן את העמדה/המחשב.

שימוש בפלטפורמות אלו על יתרונותיהן, טומן בחובו גם אתגרים אבטחתיים המיוחדים לו, הנובעים ממספר סיבות מרכזיות:

- הרחבת הפעילות במרחב הדיגיטלי תוך צמצום הצורך בממשקים פיזיים.
- תלות הולכת וגוברת של ארגונים בקיום תשתית דיגיטלית ראויה לביצוע פעולות שגרה.
- לעיתים קרובות תמיכת ה-IT מתקבלת מגורם שלישי (בעל הפלטפורמה) מחוץ לארגון. נוצרת סיטואציה של גורם מחוץ לארגון המקבל אחריות על אבטחת המידע הנמצא במערכות התשתית אשר ברשות הארגון.
- חציית סמכויות שיפוט באופן ה"שקוף" למשתמשים, כאשר כל סמכות משפטית עשויה לדרוש עמידה בדרישות אבטחה ופרטיות שונות, ולעיתים אף מתנגשות.
- עצם התקנת הפלטפורמה על עמדת קצה בארגון, מגדיל את משטח התקיפה הפוטנציאלי. לדוגמה, התוכנה עשויה להתחבר לשרת הניהול שנמצא בענן באופן עיתי לשם ביצוע פעולות ניהול/עדכון, או שהתוכנה נמצאת במצב המתנה וזאת במטרה לאפשר חיבור מרוחק, ובכך מאפשרת לתוקף פוטנציאלי ליצור אינטראקציה עם התוכנה.

מטרת המסמך

להציג ניתוח איומים בהקשר השימוש בפלטפורמות גישה מרחוק, על מנת לאפשר למקבל ההחלטות לבצע ניהול איומים מושכל בהטמעה ושימוש במערכות אלו.

מבנה המסמך

- הסבר אודות מהי פלטפורמת גישה מרחוק ודרכים שונות לשימוש.
- פרקים המנתחים סיכונים שונים בשימוש בפלטפורמה.
- פרק המלצות המתייחס הן לבחירת הפלטפורמה והן לשימוש נכון בפלטפורמה.

תיחום

- המסמך בוחן את הפלטפורמות כולן - ללא התמקדות בפתרון של יצרן ספציפי.
- המסמך בוחן את העקרונות הטמונים בבסיס השימוש בפלטפורמות אלו ולא פערים אבטחתיים הנובעים מפיקוח של פלטפורמות אלו.
- המסמך סוקר פערים אבטחתיים פוטנציאלים ומציג עקרונות מומלצים ליישום לשם שיפור רמת האבטחה.

קהל יעד

- מנהלי מערכות מחשוב, CISOs וגורמי הגנה ארגוניים.
- אנשי IT חיצוניים, הנותנים שירות לארגון.

הערה: המסמך נכתב על סמך מקורות גלויים, ללא התקנה בפועל של תוכנות מסוג השתלטות מרחוק וללא ביצוע של בדיקות חוסן מול מערכות אלו.

פלטפורמות גישה מרחוק

פלטפורמות גישה מרחוק מאפשרות קבלת סיוע מגורמי IT ללא צורך בהגעה פיזית למשרד/למעבדת תיקון.

אופן השימוש

ניתן להשיג גישה מרחוק באמצעות ארבע גישות טכנולוגיות שונות:

1. **תצורה עבודה - שימוש בשרת מתווך הנמצא בענן (Cloud)**

2. **תצורת עבודה - שימוש בשרת מתווך הנמצא ברשת המקומית (On-Premises)**

3. **תצורת עבודה - עמית לעמית (P2P) ברשת המקומית (On-Premises)**

4. **תצורת עבודה - עמית לעמית (P2P) באמצעות רשת האינטרנט**

שימוש בפלטפורמה כבסיס לתקיפה

לצד היתרונות הבולטים, השימוש בתוכנות השתלטות מרחוק מייצר לתוקף הזדמנויות לביצוע תקיפות. להלן מיפוי התקיפות ביחס לשלב במחזור החיים:

- **<u>שלב הורדת הפלטפורמה :</u>**
  - הורדת התוכנה מ**מקור לא מהימן**. הדבר נכון הן לגורם המספק תמיכה והן לבעל עמדת הקצה (המקבל את התמיכה).
  - חברות רבות המוכרות מוצרים מקצועיים של תוכנות השתלטות מרחוק, מציעות באינטרנט מוצרים במחירים נמוכים או בחינם. משתמשי קצה בארגון עלולים להתקין ישירות מוצרים אלו לשולחן העבודה שלהם, מבלי לקבל אישור מהחברה/ארגון (Shadow IT)[1], תוך חוסר ידיעה מהי רמת האבטחה במוצרים אלו, ומבלי לדעת מה הסיכונים האפשריים.
  - הורדה של התוכנה עם **תוספות לא חיוניות**, אשר עשויות להגדיל את משטח התקיפה או ליצור התנגשות עם אמצעי האבטחה הקיימים בארגון.

- **<u>שלב ההתחברות:</u>**
  - בכדי לאפשר לתומך IT לטפל בתקלה מרחוק, תוכנות ההשתלטות דורשות לפעול תחת הרשאות גבוהות. משתמשים עלולים לאפשר לצד שלישי זדוני לשלוט במחשבים שלהם ע"י **מתן פרטי ההתחברות לגורם הלא נכון** בהיסח דעת, או עקב שימוש הצד השלישי בשיטות תקיפה מסוג הנדסה חברתית (דיוג במגוון סוגים). גורם כזה יקבל שליטה מלאה בעמדת הקצה, ואף עלול להשתמש בה כ"ראש גשר" לחדירה לארגון כולו. לכן, יש לשים לב למי נותנים את הגישה, ולתקשר עם הגורם שאליו פרטי ההתחברות מגיעים, בעת ההתחברות. זאת, על מנת לוודא שאכן מדובר בתומך IT לגיטימי, שמאושר ע"י הארגון.
  - גורם חיצוני עשוי לנצל הרשאות גישה ולהתחבר, וזאת ללא ידיעתו של המשתמש. לדוגמה, גורם IT חיצוני אשר קיבל את פרטי הגישה באופן לגיטימי ומנצל אותם למטרות לא לגיטימיות לאחר שכבר סיים את תיקון התקלה במחשב.
  - פלטפורמת השליטה מרחוק עשויה ליזום פעילות ללא ידיעת הארגון, וזאת תוך מיסוך הפעולה והצגתה כלגיטימית, בעוד היא עשויה לבצע הדלפת מידע באמצעות ניצול ערוץ סמוי או באמצעות דרך אחרת.

[1] <u>Shadow IT</u>- מונח זה מתייחס למערכות תקשוב (IT) הנמצאות בשימוש בארגון במקומות שונים, ושלא אושרו ע"י גוף ה-IT של הארגון (בפועל, עקיפת סמכותו של גוף ה-IT).

- **<u>בזמן השימוש:</u>**
  - בעת עבודה מול האינטרנט, מאוד קשה לאמצעי אבטחה לוודא האם מדובר בפעילות לגיטימית של המשתמש, או האם מדובר בתוקף שמסווה את הפעילות ע"י מיסוך כפעולת שליטה תמימה.
  - חלק מהפתרונות בשוק עושים שימוש בטכנולוגיה היוצרת קשר דו-כיווני (דוגמת WebSocket[2]), דבר המאפשר לגורם התומך להעביר ביוזמתו מידע לרשת הארגון ו/או לבצע פעולות ללא ידיעת המשתמש.
  - מכיוון שכעת ישנו גורם נוסף (בעל השליטה מרחוק) שעובד על המחשב, קיימת אפשרות שגורם נוסף (שלא תכננו שיקבל גישה מרחוק) ישתמש באפשרות של גישה מרחוק ויתחבר גם הוא למחשב (Session Hijacking). במקרה זה התוקף עשוי לבחור לתקוף את בעל המחשב לשם גניבת פרטי ההתחברות או לחילופין, לתקוף במישרין את הגורם המספק תמיכה, וממנו להגיע לבעל המחשב.
  - בעל הגישה מרחוק עלול להיות חשוף בעצמו לפריצה דרך האינטרנט, ובכך הוא עלול לחשוף את רשימת הגורמים ופרטיהם (דוגמת כתובת ה-IP) אשר אושר להם בעבר להשתלט על המחשב.
  - דלף מידע, כדוגמת העתקת מידע ללא ידיעת בעל המחשב, למחשב גורם התמיכה או למחשב של גורם אחר. בנוסף, במקרים רבים הפלטפורמה ממפה כברירת מחדל את הכוננים המקומיים של בעל המחשב, וחושפת את תוכנן לגורם התמיכה - דבר אשר יכול לסייע לתוקף.
  - היעדר תיעוד מספק מונע אפשרות לביצוע תחקור בדיעבד של אירוע סייבר.

- **<u>קיומה של פלטפורמה על המחשב, אך ללא פעילות יזומה ע"י בעליו</u>**

איום פנימי, דוגמת איש תמיכה, עשוי לנצל את הפלטפורמה לשם התחברות למחשב ללא ידיעת בעליו, ובכך לקבל גישה למידע ו/או הרשאות אשר הוקנו לבעל המחשב. לאור זאת יש להשתמש בפלטפורמה המחייבת "גישה בהזמנה בלבד", או לכל הפחות לבחור בפלטפורמה המחייבת את אישור בעל המחשב בזמן אמת, וזאת כתנאי סף למתן גישה.

[2] Websocket - פרוטוקול תקשורת המאפשר ערוצי תקשורת full-duplex מעל ערוץ TCP יחיד.

המלצות הגנה בהקשר פלטפורמות השתלטות מרחוק

להלן מספר המלצות לשימוש בטוח יותר בפלטפורמות שיתוף אלו. ההמלצות מחולקות לשני הקשרים:

- בחירת פלטפורמה - בחלק זה יופיעו מספר שיקולים אבטחתיים שיש לוודא כי הפלטפורמה תומכת בהן, על מנת לאפשר לארגון הגנה מיטבית.
- שימוש נכון בפלטפורמה - בחלק זה יוצגו מספר תהליכי יסוד בשימוש בפלטפורמות ומספר התנהגויות מונעות לשם מיטוב השימוש המוגן בפלטפורמות אלו.

בחירת פלטפורמות השתלטות מרחוק

- טרם רכישת הפלטפורמה, יש לוודא כי נעשה תהליך ניהול סיכונים, וזאת תוך התייחסות לדרישות החוק, רגולציה, דרישות חוזיות וצרכים עסקיים.
- יש לבחור תוכנה מספק מוכר ואמין.
- במקרים רבים קיים פער ביכולות (אבטחתיות ואחרות) בין גרסאות שונות של הפלטפורמה (תלוי תשלום). מומלץ לבחור בגרסה המאפשרת יכולות אבטחה מיטביות.
- מומלץ לבקש אישור ודגשים מהלשכה המשפטית בארגון, המתייחסים לשימוש בפלטפורמה וההשלכות הנגזרות (דוגמת הגנת פרטיות).
- מומלץ לוודא כי הפלטפורמה עושה שימוש במערכת ניהול מרכזית.
- מומלץ לוודא כי הפלטפורמה מאפשרת תחקור של אירועי עבר, דוגמת שחזור פעולות אשר ביצע גורם התמיכה. יש לתת את הדעת לדרישות תקנות הגנת הפרטיות (אבטחה מידע), תשע"ז-2017, בנושא היסטוריית שמירת לוגים.
- מומלץ לוודא כי הפלטפורמה אינה מתירה חיבור למחשב ללא קבלת אישור מקדים מצד בעל המחשב.
- מומלץ לוודא כי הפלטפורמה עושה שימוש במנגנוני קריפטוגרפיה מקובלים לשם הגנה על המידע והפעילות (Session).
- מומלץ לוודא כי הפלטפורמה מחייבת שימוש ב-MFA (Multi Factor Authentication- אימות רב שלבי).
- מומלץ לוודא את תאימות אמצעי האבטחה הקיימים בארגון, כך שניתן יהיה להבטיח כי האיומים הנגזרים מהשימוש בפלטפורמה יאותרו, יזוהו ויסוכלו.

תהליך התקנת פלטפורמה

- טרם התקנת הפלטפורמה, יש לוודא כי נעשה תהליך ניהול סיכונים, וזאת תוך התייחסות לדרישות החוק, רגולציה דרישות חוזיות וצרכים עסקיים.
- יש לוודא כי הטמעת ותחזוקת הפלטפורמה יעשו בהתאם לתהליך ניהול השינויים הקיים בארגון.
- יש להתקין את הפלטפורמה ממקור מהימן בלבד (אתר החברה הרשמי, חנות רשמית להורדת אפליקציות).
- יש לוודא כי מותקנת גרסת התוכנה האחרונה וכי התוכנה מעודכנת כנדרש.
- יש להגדיר רשימת משתמשים המורשים להתחברות מרחוק.
- יש להגביל את הרשאות המשתמשים למינימום ההכרחי הדרוש לביצוע תפקידם (need to know, least privilege).
- בשים לב להרשאות הגבוהות של הפלטפורמות והנגישות לאמצעים חיצוניים (מצלמה, מיקרופון), מומלץ לבחור על איזה ציוד להתקין את הפלטפורמה, **תוך הנחת עבודה כי היא פעילה גם בעת שלא נראית כך**.
- יש **להגביל את שעות ההתחברות** לשליטה מרחוק לשעות הפעילות בלבד, בהתאם לשעות עבודת המתחבר (ישנה אפשרות להשוות בין שעות ההתחברות לדיווח שעות העבודה).
- יש להגביל את מספר החיבורים המותרים בו-זמנית של משתמש בודד ככל הניתן.
- יש להגביל את משך הפעילות בתוכנות השתלטות מרחוק למינימום, תוך ניתוק אוטומטי לאחר 5 דקות ללא פעילות מצב המשתמש.
- הגדרת מדינות/ אזורים אשר מורשים להתחבר לארגון.
- הגדרת הגבלות גישה למשתמשים ברמת ה-AD (Active Directory Services[3]).
- הגבלת הגישה של המשתמש המרוחק רק לסגמנטים/ מערכות/ התקנים נדרשים.
- הגדרת מנגנון לאילוץ המשתמש (בעל המחשב) להחליף סיסמה אחת ל-X זמן/חיבורים. במידת האפשר אף מומלץ להשתמש ב- OTP (One Time Password - שימוש חד פעמי בסיסמה).
- הקלטת ה-Session ("פגישה") ושמירת ההקלטה ל- X חודשים.
- תחימה ל-IP (Geo Fencing) וכתובת MAC , כך שרק דרך הארגון תהיה אפשרות במידת הצורך להיכנס למערכות שליטה מרחוק (במידה שאין תמיכה ע"י גוף חיצוני לארגון).

[3] AD - חבילת כלי שירות שפותחה על ידי מיקרוסופט לניהול רשתות בארגונים.

- בדיקת התאימות האבטחתית של העמדה המרוחקת טרם החיבור (Technology Hygiene). בדיקה שאכן העמדה אינה מהווה סכנה בחיבור (בדיקת וירוסים/ נוזקות וכד').
- ככלל, יש להימנע מהתחברות למערכת רגישה באמצעות מכשירים ניידים.
- יש לזהות ולאמת באופן חד ערכי את משתמשי המערכת.
- יש לזהות ולאמת באופן חד ערכי מכשירים מהם מתבצעת התחברות.
- ככלל, יש להימנע משימוש בתוכנות השתלטות מרחוק על גבי תשתית האינטרנט שלא באמצעות שימוש ב-VPN או SDP[4].
- יש להעדיף לעשות שימוש APN (Access Point Name) סלולרי, וזאת כחלופה למתן גישה מהאינטרנט ישירות.
- מומלץ לבצע הקשחה לפלטפורמה בהתאם להמלצות היצרן או המלצות ארגון DISA/CIS.
- במקרים בהם העובדים מתחברים מהבית באמצעות הנתב הביתי, מומלץ להעביר להם את המלצות מערך הסייבר על הקשחת הנתב הביתי בקישור הבא: https://www.gov.il/he/departments/news/homerouter.

תהליך אישור גישה לשליטה מרחוק

- הזדהות חזקה - הפעלת מנגנון MFA (Multi Factor Authentication - אימות רב שלבי).
- התחברות דרך ממשק מאובטח ומנוטר.
- הפעלת ניטור מוגבר של המשתמשים המרוחקים.
- רצוי שהגישה תותנה בסיסמה ייחודית וחד-פעמית, אשר תועבר לתומך בערוץ נפרד (Out of Band- OOB) דוגמת טלפון.
- יש לתדרך את העובדים כי לפני מתן השליטה לאיש ה-IT שעליהם:
  - לבדוק בדיוק למה הם מאפשרים גישה במחשב. במידה ויש מידע שלא ירצו שאיש ה-IT יראה, חשוב לוודא שהגישה למידע זה מצריכה סיסמה או כל אימות מסוים אחר, שרק הם יודעים.
  - לבדוק האם המצלמה/הרמקול שלהם דלוק ולוודא שיש בכך צורך. יש לוודא כי בעת הפעלת מצלמה/ מיקרופון לא נחשף מידע רגיש בפני גרום התמיכה (לדוגמה - לא מופיע על הלוח או על השולחן מידע רגיש).

[4] Software Defined Perimeter - SDP. כלי להגבלת הגישה ברשת ולמתן גישה מותאמת אישית לניהול ואבטחה למערכות ברשת.

- לוודא כי המשתמש אינו חושף מידע רגיש באפליקציות שבשימושו ואשר פעילות בזמן קבלת התמיכה.
- החיבור יתבצע אך ורק ביוזמת הארגון.
- יש לקבל אישור מהארגון לפני שמוסרים את פרטי ההתחברות

- החיבור המרוחק יתבצע בעדיפות ממחשב קבוע אשר פרטיו יתועדו ב-DB (Database- בסיס נתונים) בארגון.

תהליך סיום פעילות השליטה מרחוק באמצעות הפלטפורמה

- יש לוודא שבסיום טיפול התקלה, בוצעה התנתקות מסודרת מהמחשב עליו בוצעה ההשתלטות.
- יש להסתיר את המצלמה ולכבות את הרמקול במידה והשימוש בו הסתיים.

ביבליוגרפיה

תורת הגנת סייבר לארגונים, מערך הסייבר הלאומי
https://www.gov.il/he/departments/guides/cyber_security_methodology_for_organizations_test

Gartner

PC Remote Control Security: Risks and Recommendations, Terrence Cosgrove and John Girard, Gartner, April, 2009.

The Next Generation of Remote-Control Tools Is Emerging, David M. Coyel and Terrence Cosgrove, Gartner, October, 2008.

Remote Control Technology Landscape, John Girard, Gartner, March, 2009.

NCSC
https://www.ncsc.gov.uk/blog-post/protecting-system-administration-with-pam

NIST
https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf

Microsoft
https://info.microsoft.com/ShadowIT-Registration-he.html

Techbeacon
https://techbeacon.com/enterprise-it/10-crowdsourced-alternatives-gartner-magic-quadrant-forrester-wave

*** סוף מסמך ***