

13 אוקטובר 2021
ז' חשון תשפ"ב
סימוכין: ב-ס-1390

דרכי התמודדות ומניעה של מתקפת כופרה

תקציר



1. לאחרונה בוצעה מתקפת כופרה כנגד אחד מגופי מגזר הבריאות בישראל על ידי קבוצת תקיפה.
2. מסמך זה כולל המלצות ודרכי התמודדות בעקבות אירוע זה.
3. ההמלצות מטה אינן כוללות את כל דרכי ההתמודדות מול כל האיומים האפשריים, ומומלץ להיעזר גם בפרסומים רלוונטיים כגון [תורת ההגנה 2.0](#) של מערך הסייבר הלאומי.

דרכי התמודדות



1. להלן המלצות כלליות להתמודדות עם תקיפות מסוג זה, בחלוקה לנושאים:

1. נגישות מרשת האינטרנט וגישה מרחוק לרשת הארגונית

1. צמצמו את פוטנציאל התקיפה (Surface of Attack) למינימום האפשרי. חשפו את המספר הקטן ביותר של שרתים ופורטים הדרושים למימוש הצרכים העסקיים של הארגון, ואת השאר חיסמו באמצעות חוקי Firewall ו/או חוקי ACL בנתב. בשום מקרה אין לחשוף ישירות לרשת האינטרנט את ממשקי הניהול של השרתים השונים.
2. אפשרו גישה של משתמשי הארגון ומשתמשי צד ג' (כגון ספקים) למערכות ארגוניות, רק דרך שירות כדוגמת VPN, עם הצפנה מתאימה והזדהות חזקה (MFA) עבור כלל המשתמשים, ובפרט משתמשים בעלי הרשאות גבוהות.
3. חייבו גישה דרך שירות כנ"ל לשרתי OWA (אם קיימים בארגון), ולגישה מרחוק לשרתים ועמדות קצה ברשת הארגונית, כולל ניהול שלהם מרחוק (אם נדרש). ניהול מרחוק מומלץ לבצע באמצעות Jump Box ייעודי מנוטר, המחייב הזדהות

ניתן לשתיף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

חזקה והפעילות עליו מוקלטת.

4. אם ישנן מדינות אשר ידוע לכם כי אינכם פועלים מולן, מומלץ לבחון חסימת תעבורה ממדינות אלו באמצעות מנגנון Geolocation. זה פתרון חלקי בלבד מאחר ותוקף יכול להשתמש ב-VPN שיוצא מכתובת בישראל או במדינה שמאפשרת על ידכם, ונועד יותר למנוע מטרדי רשת ממדינות אלו.

5. הקפידו על עדכון שרתים וציוד אבטחה הנגיש מרשת האינטרנט בעדכוני אבטחה המפורסמים על ידי היצרנים השונים. עקבו גם אחרי פרסומי המערך בהקשר זה, אשר בדרך כלל יעסקו בפגיעויות קריטיות שנדרשת עבורן תגובה מיידית. בדקו את העדכונים בסביבת ניסוי והתקינו אותם בסביבת ייצור מוקדם ככל האפשר. תוקפים מנצלים את פרק הזמן בין פרסום פגיעות לעדכונה אצל כל המשתמשים, על מנת להשמיש תקיפה על בסיס הפגיעות, ולתקוף ארגונים שאינם זריזים מספיק.

2. הרשת הארגונית

1. כתובות הרשת הארגונית שאינה נגישה ישירות מהאינטרנט, יהיו על פי המוגדר ב-RFC1918 (**אלא אם ברשותכם כתובות חוקיות להגדרת הרשת הפנימית**).

2. יש לבצע סגמנטציה של הרשת הפנימית על מנת להגביל גישה לשירותים ושרתים רגישים, ולהקשות על תנועה רוחבית של תוקף ברשת. **הגדרת VLANs אינה סגמנטציה**, מאחר והגדרת VLANs ללא חוקי הגבלת תעבורה בין VLANs, מיועדת לצרכים ניהוליים ולשמירה על ביצועי הרשת, ולא לצורך אבטחת, ואינה מונעת תנועה חופשית של תוקף ברשת.

3. לארגונים מתקדמים/מחמירים, מומלץ לבחון פתרונות כגון Micro Segmentation או Zero Trust Networks, ולהטמיעם.

4. ניהול הרשת (הן שרתים והן ציוד אבטחה ותקשורת) יבוצע על ידי קבוצה קטנה ככל האפשר של מנהלנים, **ממחשבים ייעודיים** שאינם נגישים לקריאת דוא"ל או לגלישה ברשת האינטרנט, ומסגמנט רשת ייעודי. שימוש בהרשאות מנהלנים יתבצע רק לצרכי ניהול ולא לכל פעילות אחרת.

ניתן לשותף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

5. המחמירים יוסיפו גישה באמצעות Jump Box מנוטר בכניסה לסגמנט זה, הכולל הזדהות חזקה (MFA), והפעילות עליו תנוטר ותוקלט.
6. יש למנוע תעבורה בין עמדות עבודה לבין עצמן. עמדות עבודה יתקשרו עם שרתים ושירותים ארגוניים להם הן מורשות בלבד. ניתן לאכוף הגדרות אלו באמצעות הגדרות בציוד התקשורת, חוקי Firewall רשתי ו-Firewall מקומי המותקן על עמדות הקצה עצמן. **מומלץ לבחון המלצות אלו בסביבת ניסוי טרם הטמעה בסביבת ייצור.** אם קיים צורך עסקי בגישה מסוימת בין עמדות העבודה, יש להגבילה למינימום הפורטים והכתובות האפשרי.
7. אם נדרשת גישה מרחוק לעמדות הקצה, כגון לצורך תמיכה על ידי ה-Helpdesk, היא תוגבל לכתובות שבשימוש ה-Helpdesk, ולאנשיו בלבד. אין לאפשר גישה מרחוק חופשית בין עמדות עבודה, ללא צורך עסקי **המחייב** זאת.

3. תוכנות, מערכות הפעלה וחומרה בשימוש הארגון

1. **באחריות הארגון** לנהל רשימת מצאי מפורטת של כל סוגי החומרה והתוכנה שבשימוש, כולל הגרסאות השונות המותקנות במערכותיו ומורשות לשימוש על ידו.
2. **באחריות הארגון** לנהל מעקב אחר פרסום עדכוני אבטחה של היצרנים השונים עבור מוצרים הכלולים ברשימה שבסעיף קטן 1 לעיל. הארגון יגדיר מדיניות הכוללת בחינה והתקנה של עדכוני אבטחה בהקדם האפשרי, ב-SLA המתייחס הן לחומרת הפגיעות והן לרגישות המערכות השונות, וכולל התייחסות לצורך בהתקנה דחופה של עדכוני אבטחה במקרה של פגיעויות קריטיות המנוצלות בפועל בעולם.
3. ארגונים מתקדמים יגדירו ויאכפו מדיניות המונעת בפועל שימוש בתוכנות שאינן מורשות על ידי הארגון, באמצעות מנגנוני Application Whitelisting.
4. ארגונים יתקינו מערכות מסוג AV ו-EDR על עמדות הקצה והשרתים הארגוניים. האירועים ממערכות אלו ידווחו למערכת מרכזית, ויטופלו בהתאם לחומרתם, חריגותם וכו'.

5. עמדות קצה ושרתים יוגדרו כך שלא ניתן לחבר אליהם מדיה חיצונית כלשהי ולהעביר אליהם קבצים ממנה. הכנסת קבצים לרשת הארגונית תתבצע באופן ממוכן ומרוכז באמצעות עמדות הלבנה ייעודיות (כולל עבור הורדת קבצים מהרשת), וכן באמצעות מערכות סינון דוא"ל עבור צרופות. מומלץ להגביל את סוגי הקבצים המורשים בכניסה לרשת למינימום הנדרש לצרכים העסקיים, ולוודא בכל הדרכים האפשריות כי קובץ הנחזה כסוג מסוים, הוא אכן כזה.
6. מסמכי Office מרשת האינטרנט ייפתחו תמיד תחת Protected View וללא הפעלה של Macros. באופן דומה יש לנטרל הפעלת JavaScript בקבצי PDF.

4. הזדהות

1. ככל הניתן, ובפרט למשתמשים בעלי הרשאות גבוהות כגון מנהלנים, ההזדהות לרשת ולשירותיה השונים תתבצע באמצעות 2 מנגנוני הזדהות לפחות (הזדהות חזקה – MFA).
2. יש ליישם מנגנון כגון LAPS לניהול סיסמאות המנהלנים המקומיים באופן מרכזי. משתמשים לא יקבלו הרשאות מנהלן מקומי אלא אם הוכח צורך עסקי בכך.

5. לוגים ו-SIEM

1. לוגים של עמדות קצה ושרתים יועברו רשתית קרוב ככל האפשר למועד היווצרם לשרת איסוף לוגים מרכזי. שרת זה ישמש בסיס למערכת SIEM ארגונית, אשר יוגדרו בה הן חוקים סטנדרטיים ומקובלים והן חוקים התואמים את תהליכי העבודה והסביבה הארגונית הספציפית על מנת להציף פעילויות חריגות ולנסות לאתר תוקפים.

6. גיבויים

1. שימרו לפחות 2 גיבויים נפרדים של המערכות הארגוניות הקריטיות.
2. מומלץ כי אמצעי הגיבוי יהיו שונים עבור 2 הגיבויים הנ"ל (לדוגמה – מדיה נתיקה וענן). אם בוחרים בגיבוי ענן, יש לוודא כי הקבצים מוצפנים בפרוטוקול מוכר ומאושר טרם העלאתם לענן.



3. וודאו כי בכל עת קיים עותק גיבוי עדכני יחסית, שאינו מקוון, ורצוי אף במיקום פיזי שונה ממיקומם של שאר הגיבויים.
4. בצעו באופן עיתי תרגול של שחזור מערכות שונות מגיבוי, על מנת לוודא תקינות הגיבוי וכן נכונות והיכרות עם נהלי השחזור שבידיכם.

מקורות



1. <https://www.gov.il/he/departments/publications/reports/ransomware>
2. https://www.gov.il/he/departments/general/cyber_security_methodology_2

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

