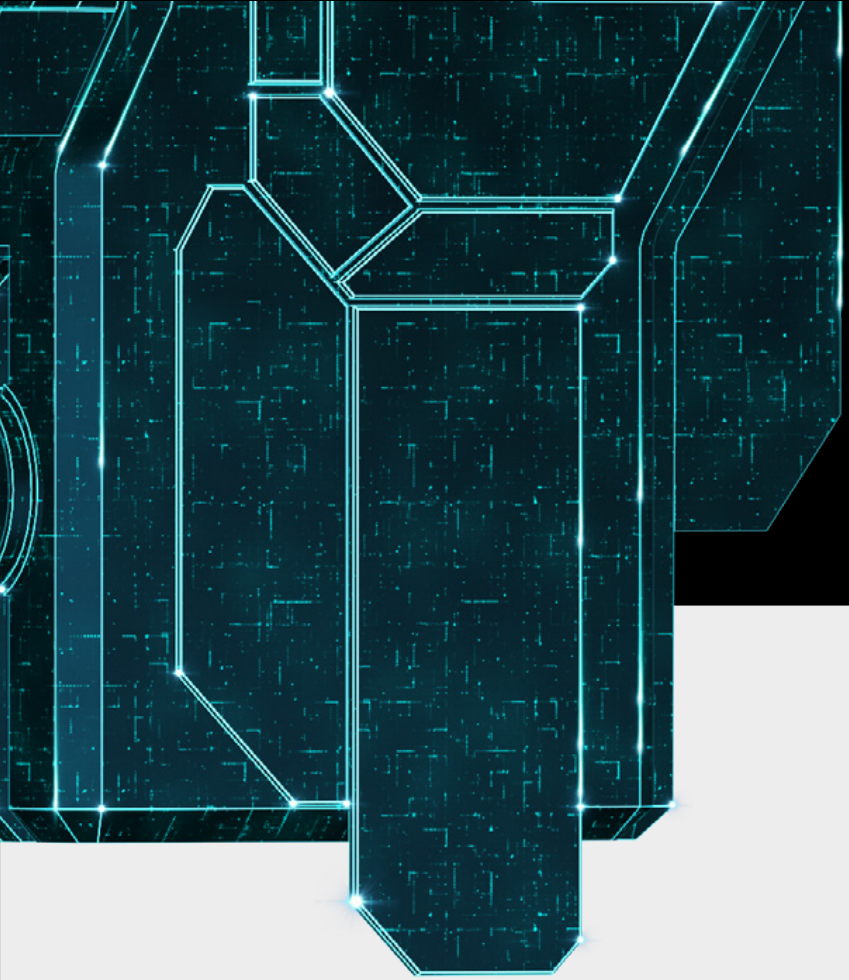


CYBERSECURITY
EXPERTS ON YOUR SIDE

RDP: הגדרות אבטחה לעתיד של עבודה מרחוק, שכלל אינו רחוק

משתמשים ב-RDP כדי לנהל את הרשת שלכם? אם כן, ודאו שאתם מצמצמים את החשיפה לאיומים באמצעות שימוש בפרקטיקות נכונות, בכלי אימות מהימנים וניצול הידע הקיים בנושא.

מגפת הקורונה גרמה לארגונים מכל רחבי העולם לשלוח את עובדיהם לעבוד מהבית, וכתוצאה מכך גרמה להם לנצל את כל כלי העבודה-מהבית בהם יכלו להשתמש. אחד מהכלים האלה הוא טכנולוגיית RDP (Remote Desktop Protocol), טכנולוגיה שבמהלך השנים האחרונות שימשה גם כבסיס למתקפה כנגד המשתמשים בה.

ממספר ניסיונות התקיפה שניצלו טכנולוגיה זו הוא עצום, ובמרבית המקרים התוקפים מצאו דרכים לניצול הגדרות שלא הוגדרו כראוי או סיסמאות חלשות כדי לקבל גישה לרשתות החברה.

מרגע שהתוקפים נכנסו, הם יכולים לעשות כמעט הכל, למשל – לגנוב נכסים קריטיים או נתונים רגישים אחרים, ולהצפין אותם על מנת לדרוש עבורם כופר.

צוות שירות ותמיכה ESET ישראל
יולי 2020

1. איך תוקפים מנצלים את פרוטוקול RDP?

בשנים האחרונות חברת ESET זיהתה מספר הולך ועולה של תקריות בהן תוקפים התחברו מרחוק לשרתי Windows שזמינים ברשת ומשתמשים בפרוטוקול RDP, ונכנסו אליו כ-Admins. לאחר שהתוקפים הגיעו ליעד הזה הם יכולים להשתמש בשיטות תקיפה מגוונות, ביניהן: פרצות אבטחה (כמו BlueKeep CVE-2019-0709), מתקפות פישינג, מתקפות מסוג: Credentials Stuffing, Password Spraying, Brute-Force, או ניצול של הגדרות גישה לא נכונות למערכות פנימיות.

לאחר שהתוקפים מתחברים לשרת כ-Admins, הם יבצעו תצפית מסוימת כדי להבין מה תפקידו של השרת, מי משתמש בו ומתי. לאחר שיהיה להם את המידע הזה, הם יוכלו להתחיל בביצוע פעולות זדוניות.

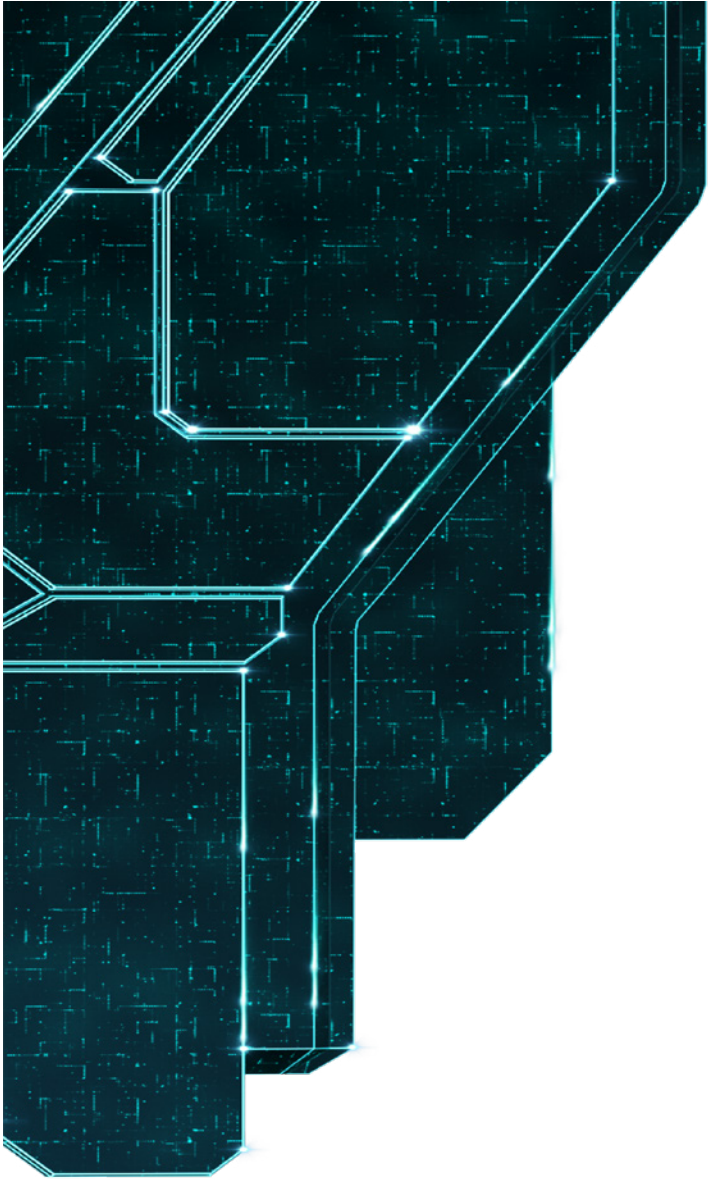
הרשימה מטה לא כוללת את כל הפעולות שהם יכולים לבצע, וברוב המקרים הם לא יבצעו את כולן. יש שוני רב בתדירות הפעולות, סדרן ואופיין בין תוקפים שונים.

בין פעולות הזדוניות שזיהינו:

- **ניקוי קבצי יומן (לוגים) שמתעדים את נוכחותם במערכת**
- **ביטול גיבויים אוטומטיים ו- Shadow Copies**
- **ביטול תוכנות אבטחה או הגדרת כללי החרגה בתוכנות אלה (פעולות שרק Admin רשאי לבצע)**
- **הורדה והתקנה של תוכנות מסוגים שונים בשרת**
- **מחיקת גיבויים ישנים או דריסתם, אם ניתן לגשת אליהם**
- **הוצאת נתונים מהשרת**

שלוש הפעולות הנפוצות ביותר הן:

- **התקנת תוכנות לכריית מטבעות במטרה ליצור מטבעות דיגיטליים (למשל Monero)**
- **התקנת כופרות במטרה לסחוט כסף מהארגון - כסף שיועבר ברוב המקרים באמצעות מטבע וירטואלי כמו ביטקוין**
- **בחלק מהמקרים, התוקפים יתקינו תוכנות נוספות לשליטה מרחוק כדי לשמר את יכולת הגישה לשרתים שכבר נפרצו (עקביות), למקרה שהפעולות שביצעו באמצעות ה-RDP יתגלו ויסוכלו**



מתקפות בולטות שמשתמשות בפרוטוקול RDP

אחת הכופרות המוצלחות ביותר, GandCrab, שהייתה פעילה עד מאי 2019, השתמשה במודל עסקי של תוכנת כופר כשירות (Ransomware as a Service, RaaS), שבו המפתחים השתמשו במספר גורמים זדוניים נוספים כדי להפיץ את הנוזקה שלהם באופן מוצלח יותר. GandCrab כיוונה את מתקפותיה אל ספקי שירותים מנוהלים (MSP) המשתמשים בפרוטוקול RDP כדי להתחבר לכלי הניהול מרחוק שלהם, וכך יכלה לסחוט כמה משתמשי נקודות-קצה במקביל.

על אף שמפעילי הנוזקה GandCrab הכריזו על פרישתם לאחר שה-FBI שחרר מפתחות המאפשרים את שחזור הצפנת הכופרה שלהם, המומחים שלנו מעריכים שקוד המקור של GandCrab נמכר לקבוצה אחרת שמפעילה כעת את הכופרה Sodinokibi (בשל שינויים בקוד, במבנה שלו ובעדכונים שקיבל). Sodinokibi החלה להופיע מעט לאחר ההכרזה על השעיית הפעילות של GandCrab. הכופרה, שלמעשה מחליפה את GandCrab, משתמשת בטקטיקות, טכניקות ופרוצדורות דומות לאלו של קודמתה, ומתקפותיה מכוונות לספקי שירותים מנוהלים המשתמשים בפרוטוקול RDP.

הקשר לספקי השירותים המנוהלים הוא בעל משמעות גם לעסקים גדולים, שכן אותם ספקי השירות מחזיקים ב"מפתחות לשער" של אלפי עסקים קטנים-בינוניים (ושל חלק מהקשרים העסקיים של אותם עסקים), ואף של כמה עסקים גדולים. הבעיה הזו קיימת גם בצד הלקוח של ספק השירותים המנוהלים, שכן שני הצוותים ושאר המשתמשים תלויים ב-Admins בכל הקשור לחידוש רישיונות, עדכוני אבטחה ועוד.

פרצה ב-RDP פותחת פתח גדול לסיכון

כמות המתקפות המשתמשות בפרוטוקול RDP גדלה בצורה איטית אך יציבה, והיא נחקרה ע"י כמה גופי ביטחון ממשלתיים בעולם, ביניהם ה-FBI, ה-NCSC הבריטי, ה-CCCS הקנדי, ה-ACSC האוסטרלי ועוד רבים נוספים. האירוע המשמעותי ביותר קרה במאי 2019 עם הופעתה של פרצה CVE-2019-0708, הידועה גם בשם "BlueKeep" – פרצה בפרוטוקול RDP המשפיעה על המערכות הבאות: Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 ו-Windows Server 2008 R2.

אמנם מדובר במערכות ישנות שברוב המקרים אינן זוכות לתמיכה כלל או זוכות לתמיכה מוגבלת מצד היצרן, נתוני הטלמטריה מראים שהרבה מערכות פגיעות כאלה עדיין נמצאות בשימוש.

פרצת BlueKeep מאפשרת לתוקפים להריץ קוד תוכנה חיצוני על מחשבי הקורבנות שלה. אף על פי שתוקפים בודדים יכולים להפיץ את מתקפתם באופן נרחב באמצעות כלי תקיפה אוטומטיים, הפרצה הזו מוגדרת כ"פרצת תולעת"– מתקפה שיכולה להפיץ את עצמה באופן אוטומטי בין רשתות ללא כל התערבות מצד המשתמשים, כמו במקרה של תולעת Win32/Diskcoder.C (המוכרת גם בשם NotPetya) ותולעת Conficker שפעלו בעבר.

ESET מציעה כלי זיהוי חינמי לפרצת (BlueKeep) CVE-2019-0709 שמאפשר לזהות מערכות הפגיעות לפריצה באמצעות פרוטוקול RDP. לחצו על הקישור הבא כדי לגלות כיצד להשתמש בו ולהוריד עותק למחשבכם (הורד) כפתור: לקריאת המאמר והורדת כלי הזיהוי

לקריאת המאמר והורדת כלי הזיהוי

*שימו לב: דווח כי גרסאות Windows 8 ואילך לנקודות קצה וגרסאות Windows Server 2012 ואילך לשרתים אינן פגיעות לפרצה זו נכון למועד פרסום הכתבה.

ניצול של פרצות תולעת נחשב ברוב המקרים לבעיה חמורה. מיקרוסופט נתנה לפרצה זו את דירוג האבטחה הגבוה ביותר, קריטי, בהנחיה שאותה פרסמה עבור לקוחותיה. בסיס הנתונים הלאומי לפרצות אבטחה של ממשלת ארה"ב דירג את הפרצה CVE-2019-0709 בניקוד 9.8 מתוך 10.

מיקרוסופט פרסמה פוסט בבלוג שלה בו המליצה בחום למשתמשים להתקין את עדכוני האבטחה שלה, גם עבור מערכות הפעלה שיצאו מתמיכה כמו Windows XP ו-Windows Server 2003. החששות בנוגע לפרצת התולעת הזאת היו כה גבוהים עד כדי כך שמועצת הביטחון הלאומית של ארה"ב (NSA) פרסמה באופן נדיר מסמך המלצה הממליץ על התקנת עדכון האבטחה של מיקרוסופט כדי לפתור את הפרצה.

למרות שהפרצה נחקרה ע"י מספר גורמי בדיקת חדירות ברחבי העולם, לא דווח על ניצול משמעותי של פרצת BlueKeep עד נובמבר 2019, אז החלו להתפרסם אין-ספור דיווחים על שימוש בפרצה, בין היתר במגזינים ZDNet ו-WIRED. המתקפות לא דווחו כמוצלחות, שכן ב-91% מהמקרים המחשבים שנפגעו קרסו עם תקלת עצירה (בדיקת באגים / מסך כחול) כשהתוקף ניסה לנצל את פרצת BlueKeep. עם זאת, ב-9% הנותרים, בהם המתקפה דווקא כן הצליחה, התוקפים הצליחו להתקין תוכנה לכריית מטבעות Monero. אף על פי שהמתקפה לא הצליחה כמתקפת תולעת, קבוצת פשיעת הסייבר הפכה את תהליך ניצול הפרצה לאוטומטי, למרות סיכויי ההצלחה הנמוכים של תהליך זה.

מכיוון שבמקרה שלנו הזמן הוא הכול, אנו נימנע מתיאור מפורט מדי של הפרצה, ובמקום זאת נתמקד בצעדים הנדרשים להגנה על רשתות מפני האיום הנובע ממנה.

.2
הגנה מפני מתקפות המנצלות את פרוטוקול RDP

מה אתם יכולים לעשות? הדבר הראשון שעליכם לעשות הוא להפסיק באופן מוחלט נגישות לשרתים שלכם דרך האינטרנט, בפרוטוקול RDP, או לפחות לצמצם את מספר ההתקשרויות למינימום האפשרי. ההנחיה הזו עשויה להיות בעייתית לעסקים רבים, במיוחד בזמנים אלה בהם רבים מהעובדים עדיין עובדים מהבית בשל מדיניות חדשה בעקבות מגפת הקורונה.

בואו נבהיר – אם אתם עדיין משתמשים ב-Windows Server 2008 או ב-Windows 7 (מערכות שהפסיקו לקבל תמיכה מינואר 2020) ומחזיקים מחשבים או שרתים שמשתמשים במערכות האלה ונגישים באופן ישיר על גבי פרוטוקול RDP, אתם נמצאים בסיכון גבוה למתקפה ועליכם לנקוט בצעדי מניעה באופן מיידי. שימוש במערכות אלה מגדיל את משטח ההתקפה שלכם באופן משמעותי, **וההמלצות מטה אמורות להבהיר לעסק בו אתם עובדים שעליו להתקדם למערכות שנתמכות באופן מלא ע"י יצרניהן.**

עבור אלו מכם שמשתמשים במערכות מעודכנות, המצב הנוכחי לא אומר שעליכם להפסיק באופן מיידי את השימוש בפרוטוקול RDP. עם זאת, עליכם לנקוט בצעדים נוספים כדי לאבטח את המערכות שלכם, באופן מהיר ויסודי ככל האפשר. כדי לסייע לכם בכך, יצרנו את **12 הצעדים החשובים ביותר להגנה על מחשבים מפני מתקפות מבוססות RDP.**

12 טיפים להגנה מפני מתקפות מבוססות RDP

ההמלצות מסודרת ע"פ מידת החשיבות של הבעיה וקלות ההטמעה של הפתרון, אך הנתונים האלה הם שונים בין ארגון לארגון. חלק מהצעדים לא יהיו ישימים בחלק מהארגונים, ובחלקם ייתכן שעדיף יהיה להטמיע באופן אחר מזה שצוין פה. ייתכן שהארגון שלכם יצטרך לנקוט בצעדים נוספים.

	המלצה	סיבה
.1	מנעו התחברויות חיצוניות למחשבים מקומיים על גבי פורט 3389 (TCP / UDP) בחומת האש הראשונית. כברירת מחדל, פרוטוקול RDP פועל על פורט 3389. אם שיניתם את ההגדרה לפורט אחר, עליכם לחסום את הפורט שבחרתם.	השארת פורטים פתוחים להתחברות מחוץ לרשת באמצעות RDP מאפשרת גישה פשוטה לתוקפים לחדירה לרשת הארגונית.
.2	בחנו והפיצו עדכון אבטחה לפרצה - BlueKeep (CVE-2019-0709) ואפשרו אימות ברמת הרשת (Network Level Authentication) במהירות האפשרית.	התקנת עדכון האבטחה של מיקרוסופט על מחשביכם ומעקב אחר הקווים המנחים שלהם מבטיח שהמחשבים יהיו מוגנים מפני פרצת BlueKeep
.3	דרשו הגדרת סיסמאות מורכבות וחזקות (סיסמה ארוכה הכוללת 15 תווים לפחות ואינה כוללת ביטויים הקשורים לשם העסק, לשמות מוצריו או לשמו של המשתמש) לכל המשתמשים שיכולים להתחבר דרך RDP.	הצעד מגן מפני מתקפות ניחוש סיסמה ו- Credential Stuffing. קל מאוד להפוך את המתקפות האלו לאוטומטיות, וחיזוק הסיסמה הופך את המשתמשים למוגנים בהרבה מפני סוג המתקפות האלו.
.4	השתמשו בסיסמאות ייחודיות לחשבונות מקומיים שניגשים לשרתים (למשל, באמצעות LAPS או בשירות ניהול סיסמאות חזק) *בנוסף: הגבילו את הרשאות הגישה לשרת לקבוצה מוגבלת של משתמשים.	מקטין את משטח ההתקפה של השרתים באמצעות צמצום מספר המשתמשים שיכולים לגשת אליו.
.5	הגדירו את רמת ההצפנה של חיבור ה-RDP ל"גבוה", במידת האפשר. אם אין אפשרות, הגדירו את רמת ההצפנה לרמה הגבוהה ביותר האפשרית.	שימוש בהצפנת 128 ביט לכל ההתקשרויות בין שרת ללקוח, במידת האפשר.

.6	התקינו פתרון אימות רב-שלבי (MFA), כמו ESET Secure Authentication (ESA), ודרשו מכל החשבונות שמסוגלים להתחבר ל-RDP ומכל חשבונות המנהל להשתמש בו.	דרישת שכבת אימות נוספת באמצעות טלפון נייד, אמצעי פיזי או מנגנון אחר, שזמינה רק לעובדים ותשמש אותם להתחברות למחשביהם.
.7	התקנת שער (gateway) ב-VPN (רשת פרטית וירטואלית) לניהול כל תקשורות ה-RDP מחוץ לרשת המקומית שלכם.	מונע תקשורות RDP בין האינטרנט ובין הרשת המקומית שלכם. מאפשר לכם לאכוף דרישות אימות וזיהוי מחמירות יותר עבור גישה מרחוק למחשבים.
.8	באמצעות מסך ניהול האבטחה שלכם, וודאו שפתרון האבטחה לנקודות הקצה שלכם, המוגן ע"י סיסמה, משתמש בסיסמא חזקה שאינה קשורה לחשבונות אדמיניסטרטיביים ולחשבונות שירות. ESMC (ESET Security Management Center) מאפשר לשלוט בניהול המדיניות באופן פשוט אך מעמיק, ומאפשר ליצור קבוצות מחשבים שונות עם מדיניות שונה לכל קבוצה. בנוסף, ניתן להשתמש ב- ESMC מכמה מחשבים שונים (Multitenancy) וניתן לגשת אליו באמצעות התחברות מאובטחת ע"י מנגנון MFA.	מספק שכבת אבטחה נוספת למקרה שתוקף מקבל גישה למשתמש עם הרשאות מנהל ברשת שלכם.
.9	אפשרו חסימת פרצות - טכנולוגיית זיהוי אנומליות שאינה מבוססת חתימה - בתוכנת האבטחה לנקודת הקצה שברשותכם, שמנטרת את התנהגותן של תוכנות המשמשות כבסיס למתקפות בדרך כלל.	רבות מתוכנות האבטחה לנקודות קצה יכולות לחסום גם טכניקות לניצול פרצות. וודאו שפונקציה זו מאופשרת.
.10	בודדו מחשבים לא-מאובטחים שניתן לגשת אליהם באמצעות פרוטוקול RDP.	השתמשו בטכניקות בידוד ברשת שלכם כדי לחסום מחשב (או מחשבים) פגיע מיתר הרשת.
.11	החליפו מחשבים לא-בטוחים.	אם לא ניתן להתקין במחשב עדכון אבטחה (כנגד פרצת BlueKeep), התכוננו להחלפתו הקרבה ובאה.
.12	שקלו שימוש בחסימת GeoIP בשער ה-VPN שלכם.	אם עובדי החברה וספקיה נמצאים באותה המדינה או ברשימה מצומצמת של מדינות, שקלו לחסום את הגישה ממדינות מסוימות כדי למנוע התחברות של תוקף ממדינה זרה.

3.
כיצד ESET מסייעת לכם להתגונן מפני פרצות ב-RDP

הצעד הראשון עליו אנו ממליצים הוא לוודא שתוכנת אבטחת נקודת הקצה שלכם מעודכנת ומזהה את פרצת BlueKeep. לטכנולוגיה הרב שכבתית של תוכנת האבטחה של ESET יש תפקיד משמעותי. BlueKeep מזוהה כ- CVE-2019-0708 RDP / Exploit במודול ההגנה מפני מתקפות רשת של ESET, שהוא הרחבה של טכנולוגיית חומת האש של ESET שנמצאת במוצרי אבטחת נקודות הקצה של ESET מגרסה 7 והלאה.
שכבת טכנולוגיה נוספת שחשובה להגנה על פרוטוקול RDP היא חוסם פרצות האבטחה של ESET, שמנטר אפליקציות שפרצותיהן מנוצלות באופן תכוף (דפדפנים, מעבדי תמלילים, תוכנות דוא"ל, Flash, Java ועוד). במקום לנסות ולאתר רק מזהי CVE, טכנולוגיה זו מתמקדת בטכניקות ניצול הפרצה. כאשר השכבה מזהה פעילות חשודה היא מתעוררת והאיום נחסם באופן מיידי באותו המחשב.

במקביל לטכנולוגיה זו, אנו ממליצים לכם להטמיע נהלים שיהיו ידידותיים למשתמש ככל האפשר – נהלים שיהפכו לקלים אף יותר באמצעות שימוש בכלים פשוטים לשימוש. אבטחת פרוטוקול RDP דורשת מספר צעדים (פרוצדורליים), אך שימוש במנגנון אימות רב-שלבי (MFA) פשוט הוא השלב החשוב ביותר, שכן הוא משמש כהגנה מפני סיסמאות קלות לניחוש ומפני מתקפות Brute Force. התמקדות באימות לפני גישה למערכת או פלטפורמה, כמו RDP במקרה שלנו, מגנה על אחת מהמערכות החשובות ביותר לניהול אבטחת הרשת והמשתמשים שברשות העסק שלכם.

פתרון ה-MFA שלנו, ESA (ESET Secure Authentication), מגן על צורות תקשורת פגיעות כמו RDP באמצעות הוספת אימות רב-שלבי להתחברויות אלה.

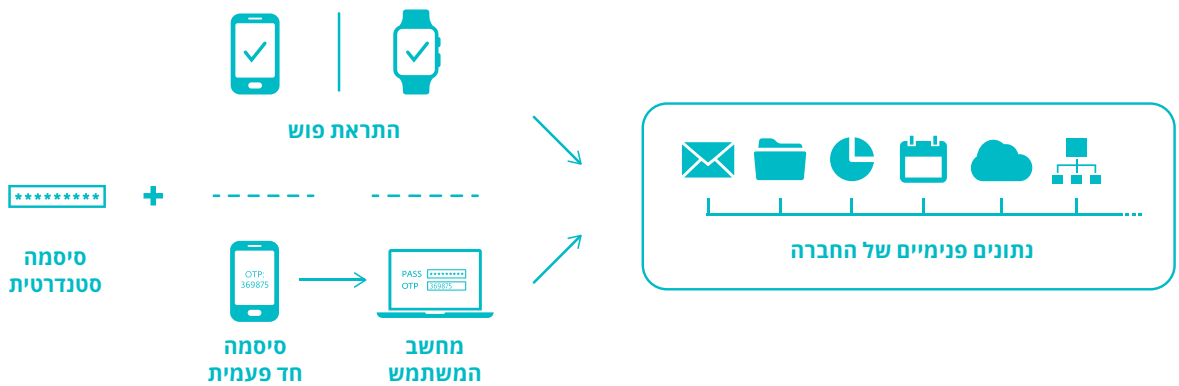
פתרון כמו ESA תומך בכל רשתות ה-VPN (כלי אבטחה נוסף להגנה על רשתות), מתחבר לכל המכשירים הקריטיים שכוללים מידע רגיש ולשירותי ענן כמו Office 365, Google Apps ו-Dropbox, וכן לשירותים אחרים המשתמשים ב- ADFS 3.0 או ב- SAML.

פתרון ESA, שמנוהל באופן מרכזי מהשרת, תוכנן כך שיעבוד על כל מכשירי iPhone ו-Android, והוא פועל עם שורה ארוכה של אמצעי אימות כמו התראות פוש, אפליקציות ניידות, אמצעי אימות פיזיים, מפתחות FIDO ושיטות אימות מותאמות-אישית אחרות (על פי ה-SDK של ESA). באותו הזמן, ההגנה של ESA על הנתונים שבמחשבי החברה ועל הנתונים שבשירותי הענן שלה באופן פשוט אך עוצמתי מאפשר עמידה בדרישות התקינה העכשוויות כמו GDPR.

במיוחד בתקופה בה הרגלי העבודה משתנים חשוב שחברות יאבטחו את המערכות הקריטיות והמידע הרגיש שברשותם באופן יעיל ופשוט, חברת ESET מציעה גרסת ניסיון ל-30 יום לפתרון ה-MFA

למידע נוסף והורדת גרסת ניסיון

הוספת פתרון הצפנה כהמשך ל-MFA היא צעד חשוב נוסף. EFDE (ESET Full Disk Encryption) מאפשר הצפנה חזקה של כונני מערכת, מחיצות או כוננים שלמים. כל אלה מנוהלים באופן טבעי ע"י קונסולות הניהול של ESET, ESET Security Management Center ו-ESET Cloud Administrator, מה שמשפר עוד יותר את אבטחת הנתונים בארגון שלכם.



ידע הוא כוח. גם הגנה מקיפה היא כוח.

ניתן לבחון מספר רב של טכניקות וטקטיקות שונות לניצול פרוטוקול RDP בבסיס המידע של MITRE ATT&CK®. בסיס המידע הזה אמנם מתבסס על ממצאי מחקריהם של חברות אבטחה שונות, אך הוא מביא את כל הנתונים האלה למרחב משותף אחד. שימוש ב-ATT&CK ובכלים שונים (כלי EDR) עשוי לסייע לכם מאוד בבחינה מדוקדקת של האיומים העומדים בפני הרשת שלכם.
כלים כמו (ESET Enterprise Inspector) EEI מאפשרים למנהלי אבטחה לבחון זיהויי מתקפות ולקבל הפניה ישירה לבסיס המידע של ATT&CK לקבלת מידע נוסף ולהגדרת התראות מותאמות אישית עבור הרשת שלכם.

כשמדובר במתקפות על בסיס RDP, ישנה אפשרות נוספת – ייתכן שקיבלתם זיהויי מתקפות (חלקיים) אך נותרתם לא-מוגנים.
כלי EDR יכולים להיות שימושיים גם במקרים כאלה, בהם לא התבצע זיהוי ברור של אופי המתקפה. לדוגמה, בחלק מהמקרים פרצת BlueKeep הקריסה את המערכת המותקפת באופן מיידי מכיוון שזו הוכחה כלא-אמינה. במקרה כזה, אם התוקף רוצה שפרצת ה-RDP תמשיך לתפקד, ייתכן שהוא ירצה לחבר אותה עם פרצה נוספת, כמו פרצת הדלפת מידע (למשל, באמצעות קבצי Flash או PHP) שחושפות את כתובות הזיכרון ב-Kernel, כך שלא יהיה צורך לנחש אותן פעם נוספת. זה יכול להקטין את סיכויי הקריסה, שכן הפרצה הנוכחית מבצעת Heap Spraying רחב-היקף. ניתן לסמן את ההתנהגויות האלה באמצעות כללים מובנים שנוצרים בתוך ה-EEI, שיפעילו התראה ויסבו את תשומת ליבו של מנהל הרשת להתרחשויות. ניתן לקבל מודיעין נוסף בנוגע לרשת באמצעות בדיקת חדירות רגילה ובאמצעות בדיקת התנהגויות חשודות באמצעות IDS, IPS, SIEM.

לסיכום

מגפת קורונה שינתה את אופן העבודה של ארגונים – לא באופן זמני ורק למשך המגפה, אלא לתמיד. על המעסיקים להתאים את עצמם לא רק לדרישות הנוכחיות של העסקת עובדים מהבית, אלא גם לדרישות העתידיות של עובדים כאלה.

המגפה הזאת הוכיחה לנו שרבות מהמטלות והמשימות שבעבר נחשבו לכאלה שניתנות לביצוע רק מהמשרד יבוצעו בעתיד על ידי עובדים שעבודתם מתבצעת מרחוק. אך כדי שזה יקרה, על העובדים מרחוק להתחבר באופן בטוח למשרד. חברת ESET מציע מגוון רחב של פתרונות שיכולים לסייע לעסקים לספק גישה בטוחה לרשת הארגונית.