

# כוננות לאיומי תקיפות Cyber

תקיפות מערכות ארגוניות, הנחיות אבטחה המלצות ודרכי התגוננות

#Opisrael 2021

## הקדמה:

בשנים האחרונות קיימת מגמה גוברת של גורמים התומכים בארגוניים אנטי ישראלים ומחפשים לפגוע במדינתנו באמצעות המרחב האינטרנטי.

המתקפות מתמקדות בתקיפת כל הארגונים הנמצאים תחת ישראל, בין אם הם מספקים שירותים מרכזיים למדינה, כגון שירותים פיננסיים, אנרגיה, תעופה, טלקום וכו' ובין אם הם גופים המיצגים את מערכת הביטחון או הממשלה, בשנים קודמות נראה שהותקפו גם עסקים ישראלים פרטיים. קיימת הערכה שתבצע התארגנות למתקפה גדולה מסוג זה ביום רביעי בתאריך 07.04.2021. למבצע אשר תויג בשם המסורתי #OpIsrael מצטרפים כמדי שנה מספר קבוצות האקרים. מרבית המשתתפים במתקפה הינם האקטיביסטים שמוחים על פעילות ישראל.

השנה אנו מתמודדים במקביל עם אתגר מגפת הקורונה, שמשנה תרבויות ארגוניות עם התחברות מרחוק למשאבים ארגוניים, שיחות וידאו ועוד...

עקב כך נראית עליה במתקפות הנדסה חברתית, רכיבי תוכנה זדוניים ומתקפות על רשתות ארגוניות במטרה לאתר משאבים ארגוניים פגיעים שנחשפו לרשת האינטרנט.

## 1. המטרה המוצהרת:

ניסיון לפגוע במערכות ישראליות על ידי פגיעה בסודיות, זמינות או שלמות המידע ובכך לשבש את אורח החיים של תושבי מדינת ישראל ולזרוע בהלה.

## 2. אופי המתקפה:

מידע על אופי המתקפה לא מפורסם ולא נחשף באופן גלוי ברשת אך קיימות הערכות שונות המבוססות על אירועי עבר ועל סוגי מתקפות שאירעו בהקשרים דומים בעולם. באותו משפט נוסף ונאמר, כי היקף הפגיעה בפועל בשנים **עברו** היה נמוך יחסית וביטא את ההיערכות הטובה אליה נערכו ארגונים לקראת המתקפה. הגורמים שנפגעו היו בד"כ גופים קטנים\ בינוניים שלא נערכו והתגוננו היטב.

חשוב לנו לציין שלא ניתן לקבוע בוודאות את אופי המתקפה, את שלביה ואופי ההתפתחות שלה אך קיים סיכוי סביר שיתבצע שימוש בסוגי ההתקפות הבאים, לפי דירוג הסבירות המצוין.

### א. חדירה לרשתות ארגוניות דרך משאבים החשופים לאינטרנט **סבירות גבוהה:**

- עקב העלייה בצורך בהתחברות מרוחקת למשאבים ארגוניים, הצפי הוא כי הנושא יגרור למתקפות שונות:

- **גניבת פרטי הזדהות** – תוקפים עלולים להעזר בבסיסי נתונים שהודלפו או לבצע התקפות פשינג ממוקדות על עובדים בארגון על מנת לגנוב פרטי הזדהות ולהשתמש בהם על מנת להתחבר לרשת הארגונית. בשבועות האחרונים נראית עלייה חדה בהתקפות פשינג בדגש על כתובות שמכילות את המילים Corona או Covid-19.
- **ניצול פגיעויות ברכיבים** – ארגונים רבים מאפשרים גישה לרשת הארגונית באמצעות חיבור VPN, בהנחה והרכיבים ברשת מעודכנים לעדכוני האבטחה האחרונים ומוגנים באמצעות רכיבי אבטחת מידע, יש לוודא גם ששרת ה-VPN שבשימוש מוקשח ומעודכן לעדכוני האבטחה האחרונים.

### ב. מתקפות מניעת שירות **סבירות גבוהה:**

מתקפות אלה מיועדות למנוע אפשרות לקבלת שירות ממערכות שונות.

מתקפות אלה מתחלקות ל 3 סוגים עיקריים:

- מתקפות ברמת תשתיות ה IT (נתבים, - DNS, FW, שרתי Web עצמם, תשתית הזדהות וכו'). **ברצוננו לתת דגש מיוחד לחשש מפני מתקפות על תשתיות DNS.**
- Volume (Flood) הצפת קו תקשורת המשמש לגישה לשירות ע"י מילוי רוחב הפס.
- **מתקפה על שכבת האפליקציה Backend / מתקפות המרכוזות בחולשה באפליקציה,** לדוגמא: הרצת שאילות כבדות אשר מעמיסות את בסיס הנתונים, שאילות שמייצרות תשובות גדולות וכיוב'.

ג. השחתה ( Defacement ) של אתרי אינטרנט ואפליקציות WEB **סבירות גבוהה:**  
למתקפות מסוג זה ערך תדמיתי גבוה יותר הן לארגון והן לתוקף אך יישומן הינו מסובך יותר.  
המתקפות מאפשרות לתוקפים לשנות את תוכן האתר המוצג לגולשים וכן להחדיר באמצעותו מסרים.

ד. מתקפות סחיטה - **סבירות גבוהה:**

שימוש בטכניקות החדרה כגון: Spear Phishing או Water Hole שיובילו נעילת קבצים על ידי Ransomware או והדלפת מידע. התוקף יבקש לקבל תשלום, בד"כ במטבעות Bitcoin, על מנת לשחרר את הקבצים או למחוק את המידע שנגנב. זהו אחד האזורים הקשים ביותר לניטור כי קיים חשש שישנם כלים ייעודיים שפותחו במיוחד למתקפה הקרובה, בדרך כלל מדובר בהתקפות מתחכמות יותר שקשה יותר לצפות אותן באופן מוקדם.

ה. פרסום מידע חסוי (כרטיסי אשראי, פרטי משתמשים) **סבירות בינונית:**

ייתכן שמידע שכבר הושג בעבר יפורסם ביום המתקפה ע"מ ליצור נפח נוסף למתקפה הכוללת, מניסיון עבר חלק ניכר המידע שמפורסם אינו רלוונטי אך יש להתייחס למידע כאיום ממשי (תדמיתי וכלכלי).

## המלצות ודרכי התגוננות בפני המתקפות

ההמלצות הינן המלצות כלליות ועל הארגון לבצע הערכת סיכונים מתאימה וכן לקבוע מבעוד מועד את כלי ההתמודדות ואופי השימוש בהם. מטרת ההמלצות להעלות את רמת המוכנות להתמודדות בפני מתקפות אך אין ביכולתן לבטל לחלוטין את השפעת המתקפה או את הצלחתן.

### 1. העלאת המודעות הארגונית

- a. שליחת דוא"ל מטעם מנהל אבטחת המידע בארגון (אם קיים) או מנהל התשתיות המתריע על ההתקפה הצפויה ועל הנזק העלול להיגרם לארגון.
- b. בדוא"ל זה יש לרשום כללי עשה/אל תעשה ברורים כדלקמן:
- לא לפתוח מסמך מצורף שהגיע בדוא"ל ממקור לא מוכר
  - לא ללחוץ על קישור (Link) שהגיע בדוא"ל ממקור לא מוכר
  - לא לחבר לתחנת העבודה התקני מדיה נתיקים ( Disk on Key, CD/DVD , HDD) ממקור שאינו מהימן. (במידה וקיימת בארגון עמדת הלבנה יש להשתמש בה תמיד לפני הכנסת קבצים ממקור חיצוני)
  - לדווח למנהל אבטחת המידע/מנהל התשתיות במידה והגיע דוא"ל ממקור לא ידוע המכיל מסמך מצורף ו/או קישור (ללא פתיחת הקובץ או לחיצה על הקישור)
  - לא לפתוח מסמכים מצורפים שהגיעו בדוא"ל ממקור ידוע, אך אינם קשורים לתחום עיסוקו של הנמען
- c. לא ללחוץ על פרסומות (Banners) ולא להוריד קבצים מאתרים שאינם מהימנים.
- d. לא להוריד קבצים שאינם קשורים לתחום עיסוקו של המשתמש מאתרי אחסון ושיתוף קבצים.
- e. לא לתת פרטים מזהים בשיחה טלפונית, בדגש על שם משתמש וסיסמה. (אלא אם כן העובד מטלפן ביוזמתו לקבל תמיכה מגורם מהימן)
- f. יש לצרוך מידע בנוגע למגפת הקורונה מגורמים רשמיים בלבד:
- [https://www.gov.il/he/departments/ministry\\_of\\_health](https://www.gov.il/he/departments/ministry_of_health)
- <https://govextra.gov.il/ministry-of-health/corona/corona-virus/>
- g. לדווח באופן מיידי לגורמי הביטחון בחברה על כל אירוע חריג אחר שלא צוין במפורש.



## 2. גיבוי

- a. גיבוי מלא של כלל השרתים בארגון. (מערכת הפעלה ונתונים)
- b. גיבוי מלא של הגדרות התצורה בצידוק התקשורת. (מתגים, נתבים, מרכזיות, ציוד Wi-Fi וכו')
- c. גיבוי מלא של הגדרות התצורה במערכות אבטחת המידע הקיימות. (Firewall, IPS, WAF, SSL VPN וכדו')
- d. בדיקה וחידוד של נהלי עלייה לאוויר מ DR. (במידה וקיים אתר DR)
- e. בדיקה ווידוא כי קיימים גיבויים עדכניים ופעילים לטובת יכולת שחזור מהירה בעת הצורך.

## 3. ניהול מערכות, משתמשים, סיסמאות ועדכוני תכנה:

- a. יש להגדיר ערוצים בטוחים לחיבור למערכות ארגוניות מרחוק, לדוגמא: מערכות Web עם הזדהות חזקה, אימות דו-שלבי, ניטור ותקשורת מוצפנת (TLS). אין לחשוף פרוטוקולים כמו RDP או SMB לרשת האינטרנט.
- b. עדכון חתימות של מערכות ה-Antivirus/Anti Malware הנמצאות בשימוש בארגון. (תחנות עבודה, שרתים, דוא"ל וכו')
- c. הפצת/התקנת עדכוני תוכנה ואבטחת מידע עדכניים, ברמת חומרה "קריטי" לפחות, לכל מערכות ההפעלה לשרתים ותחנות עבודה בארגון.
- d. יש להגדיר את מערכות אבטחת המידע השונות לחסימה והתראה על דומיינים שמשייכים לאתרי פישיינג, ניתן להשתמש [ברשימה הבאה](#).
- e. אופציונאלי: שינוי סיסמאות של משתמשי מערכת בצידוק תקשורת ומערכות אבטחת מידע.
- f. אופציונאלי: שינוי סיסמאות של משתמשי מערכת מקומיים בשרתים ותחנות עבודה.
- g. אופציונאלי: חסימת גישה מבעוד-מועד לנכסי מידע ומערכות.
- h. בארגון (אתר אינטרנט שיווקי ותפעולי, שרתי דוא"ל וכו') ע"ב מיקום גאוגרפי (Geo-Location) של כתובת המקור (לדוגמא סין, רוסיה, הרשות הפלסטינית, מדינות ערביות/מוסלמיות אחרות וכדו'). הערה: במידה ולא בוצע מראש, יש לבצע באופן מיידי במידה ומתגלה התקפה.

#### 4. היערכות ארגונית

- a. הכנת רשימת בעלי תפקידים רלוונטיים, מספרי טלפון וכתובות דוא"ל לטיפול במקרה של אירוע חריג, הן של גורמים פנימיים (לדוגמא System, Helpdesk, תקשורת, אבטחת מידע וכו') והן של גורמים חיצוניים (תמיכה עסקית של ספקי האינטרנט, גורמי תמיכה במערכות שונות וכו'). יש לתקף מספרי טלפון וכתובת דוא"ל של כל גורם המופיע ברשימה.
- b. הגדרת שרשרת דיווח במקרה של אירוע אבטחת מידע כולל הגדרת רמות חומרה של אירועים שעליהם יש לדווח או להגיב באופן מיוחד\ שונה.
- c. מומלץ להתעדכן באופן שוטף באתר של ה CERT הלאומי בדבר המתקפות ואף לפנות ל CERT לסיוע התייעצות דיווח במקרה של מתקפה. ניתן לקבל פרטים ומידע נוסף בכתובת הבאה:

[https://www.gov.il/he/Departments/israel\\_national\\_cyber\\_directorate](https://www.gov.il/he/Departments/israel_national_cyber_directorate)

#### הערכות מחלקת MSSP

- 1. תגבור כוח אדם ב - SOC , הוגדרו כוננים מצוות ה-PS ואנליסטים מצוות ה SOC
- 2. חידוד נהלים במחלקה
- 3. עדכון פרטי יצירת קשר מול לקוחות בזמן אירוע אמת
- 4. הקשחת מערכות ( חסימת מדינות עוינות במערכת ה - WAF )

#### 2. כיצד חברת 2BSecure יכולה לסייע ?

- צוות IRT לטיפול באירועי אבטחה. לרשות לקוחות ה SLA שלנו יעמוד ביום המתקפה המתוכנן צוות שיוכל לתת סיוע בזמן אמת של חקירת האירוע ומתן המלצות
- **חיבור לשירותי אבטחת מידע בענן בתצורת MSSP ( Managed Security Service Providers)**
  - o שירות WAF בענן להגנה על אתרי אינטרנט בפני מתקפות.
  - o שירותי NOC - לניטור תשתיות ארגוניות ורוחב פס.
  - o שירותי SOC לניטור אירועי אבטחה במערכות אבטחה ארגוניות.
  - o שירותי EDR לניטור וחסימת מתקפות בתחנות ושרתים
- ייעוץ לגבי פיתוח והתאמה של כלי התמודדות עם תרחישי אירועים במערכות האבטחה הקיימות.

**דרכי התקשרות מחלקת MSSP:**

אנו זמינים 24/7 לכל שאלה או התייעצות.

טלפון|Whatsapp כונן SOC : 054-9497539

טלפון משרדי : 073-2256822

**דרכי התקשרות מחלקת אינטגרציה:**

המומחים שלנו ידווחו ONLINE בדף הפייסבוק של 2BSecure בהתרחשויות השונות הקשורות למתקפה.

לשאלות נוספות ניתן לפנות אלינו באמצעות המייל: [mssp@2bsecure.co.il](mailto:mssp@2bsecure.co.il)

זמינות בטלפון: באמצעות מוקד שרות בטלפון 1599.50.70.90, המוקדנית מעבירה לכוון אבטחת מידע.

בברכה,

2BSecure

