



סייבר ישראל

מערך הסייבר הלאומי

דרכי פעולה מומלצות היערכות והתמודדות עם אירוע כופרה (Ransomware) בארגון





דרכי פעולה מומלצות היערכות והתמודדות עם אירוע כופרה (Ransomware) בארגון

יוני 2021

מסמך זה נכתב ע"י מערך הסייבר הלאומי לצורך קידום הגנת הסייבר במשק הישראלי. כל הזכויות שמורות למדינת ישראל - מערך הסייבר הלאומי. המסמך נכתב כשירות לציבור. העתקת המסמך או שילובו במסמכים אחרים כפוף לתנאים הבאים: מתן קרדיט למערך הסייבר הלאומי בפורמט המופיע להלן; שימוש בגרסה העדכנית של המסמך; אי הכנסת שינויים במסמך.

המסמך מכיל מידע מקצועי, אשר יישומו בארגון מצריך היכרות עם מערכות הארגון והתאמה למאפייניו בידי איש מקצוע בתחום הגנת הסייבר.

הערות והתייחסויות למסמך ניתן להעביר למייל: tora@cyber.gov.il



תוכן עניינים <<<<

3	מבוא
4	מטרות ויעדים
4	קהל היעד
5	תיחום המסמך
5	איומים הנגזרים מתקיפת כופרה (Ransomware)
7	דרכי פעולה מומלצות - היערכות והתמודדות עם אירוע כופרה בארגון
25	נספחים
25	קיצורי שמות
26	מסמכים ישימים

««« דרכי פעולה מומלצות - היערכות והתמודדות עם אירוע כופרה (Ransomware) בארגון

1. מבוא

כופרה (Ransomware) מהווה סוג של נוזקה (Malware) אשר מטרתה לשלול מהגורם המותקף גישה לנכס הסייבר והמידע המאוחסן בו. כתנאי להסרת מגבלת הגישה, התוקף עשוי להציג תנאים שונים לגורם המותקף, דוגמת תשלום "דמי כופר". תקיפת כופרה עשויה להוות אירוע סייבר בעל משמעות נרחבת לארגונים במשק. במסגרת התקיפה, שכיח לראות כי תוקף מצפין את המידע אשר ברשות הארגון, ומתנה את הסרת ההצפנה בקבלת תגמול, דוגמת העברת כסף דיגיטלי לתוקף. ובמילים אחרות, התוקף סוחט את הארגון בדרישה לקבלת תגמול, וזאת כתנאי להסרת ההצפנה. בהינתן כי הארגון לא עמד בדרישות התוקף, וכי אין ברשות הארגון דרך אפקטיבית לשחזור המידע, לארגון עשוי להיגרם נזק בלתי הפיך, עד לכדי פשיטת רגל.

בשנים האחרונות ניתן לראות כי תוקפים במרחב הסייבר עושים שימוש במודל תקיפה מתקדם יותר בעת שימוש בכופרה - "סחיטה כפולה" (Double Extortion), כאשר המודל מבוסס על שני שלבי תקיפה עיקריים. בשלב הראשון התוקף מבצע הדלפה של מידע רגיש/חסוי מהארגון. ובשלב השני, התוקף עושה שימוש בהצפנה לשם מניעת גישה לנכסי הסייבר והמידע הארגוני, ולאחר מכן התוקף מפרסם את התנאים שלו להסרת מגבלת הגישה. יתרון מודל זה לתוקף הינו שגם אם הארגון מצליח לשחזר את המידע ונכסי הסייבר, החשש של הגורם המותקף מחשיפת המידע הרגיש/החסוי (וההשלכות הנגזרות) עשוי לדרבן אותו להיענות לדרישות התוקף.

לאחרונה התגלו מספר מקרים בהם בוצע שימוש במודל תקיפה מתקדם עוד יותר - "סחיטה משולשת" (Triple Extortion), כאשר מודל זה מבוסס על שלושה שלבי תקיפה עיקריים. בשלב הראשון התוקף מבצע הדלפה של מידע רגיש/חסוי מהארגון. בשלב השני, התוקף עושה שימוש בהצפנה לשם מניעת גישה לנכסי הסייבר והמידע הארגוני, ולאחר מכן התוקף מפרסם את התנאים שלו להסרת מגבלת הגישה. בשלב השלישי התוקף פונה לגורמי צד-שלישי (דוגמת לקוחות הארגון) בדרישה לתשלום דמי כופר כתנאי לאי פרסום מידע רגיש/חסוי שלהם או התוקף מאיים להפעיל תקיפה נוספת כנגד הארגון, דוגמת תקיפת מניעת שירות מבוזרת (DDoS), אם דרישותיו לא יענו. יתרון מודל זה לתוקף הינו שגם אם הארגון מצליח לשחזר את המידע ונכסי הסייבר, החשש של הארגון המותקף או גורם צד-

שלישי מחשיפת המידע הרגיש/החסוי (וההשלכות הנגזרות), וזאת לצד שילוב אופציונאלי של תקיפה נוספת כנגד הארגון, עשוי לדרבן היענות לדרישות התוקף.

לאור זאת, גם אם הארגון מצליח להתאושש בהצלחה מפעילות הכופרה, עדיין מתקיימת חשיפה גבוהה לארגון ולמידע של צד-שלישי (דוגמת לקוחות הארגון).

יצוין כי בשנים האחרונות החלו תוקפים במרחב הסייבר לאמץ מודל כופרה כשירות (RaaS - Ransomware as a Service), דבר המקנה לתוקפים בעלי יכולות טכנולוגיות מוגבלות או תוקפים אשר אינם מעוניינים להשקיע משאבים רבים במחקר ופיתוח, לקבל גישה לכלי תקיפה מתקדמים.

במאמר מוסגר יצוין כי ישנם מספר דיווחים מהעולם על שימוש בכופרה המממשת מספר שכבות הצפנה בלתי תלויות, כאשר כל מפתח פענוח שכבת הצפנה הינו ייחודי, וקבלתו מחייבת תשלום נפרד. בנוסף, ישנו דיווח ראשוני על התכנות קיומם של מודלים עסקיים מתקדמים יותר מצד תוקפים העושים שימוש בכופרה, דוגמת "מכירת מפתח פענוח" המותאם לפי פרמטרים דוגמת נפח מידע לשחזור, סוג קבצים הניתנים לשחזור, קצב פענוח/משך זמן פענוח צפוי, פענוח מטאדאטה (Metadata) בלבד או פענוח מידע גולמי מלא.

2. מטרות ויעדים

מסמך זה בא לסייע למנהל אבטחת מידע וסייבר / ממונה הגנת המידע והסייבר (CISO) ומקבלי ההחלטות בארגון בהיערכות והתמודדות עם אירוע כופרה בארגון.

3. קהל היעד

מסמך זה נכתב עבור מנהל הגנת הסייבר בארגון (CISO), ומקבלי ההחלטות בארגון.

גורמים נוספים אשר עשויים להפיק ערך מוסף ממסמך זה הם מנהל מערכות המידע (CIO - Chief Information Officer), מוסמך מתודולוגיות הגנת סייבר, מוסמך מיישם הגנת סייבר, מוסמך טכנולוגיות הגנת סייבר (ארכיטקט הגנה בסייבר), אנשי תקשורת נתונים/תקשוב/IT וסיסטם.

4. תיחום המסמך

המסמך "דרכי פעולה מומלצות - היערכות והתמודדות עם אירוע כופרה (Ransomware) בארגון" מתמקד בהמלצות ליישום לשם שיפור יכולת הארגון להתמודד עם אירוע כופרה. ראוי לציין כי המסמך אינו כולל הרחבה בנושאים שלגביהם מערך הסייבר הלאומי כתב ופרסם מסמכים ייעודיים. דוגמה לנושא מסוג זה הינה הגנה פרטנית על מערכת ותשתית, דבר הזוכה למענה במסגרת 'תורת ההגנה בסייבר לארגון' אשר נכתבה ופורסמה על-ידי מערך הסייבר הלאומי.

5. איומים הנגזרים מתקיפת כופרה (Ransomware)

פרק זה סוקר את האיומים העיקריים הנגזרים מתקיפת כופרה (Ransomware):

שם האיום	תיאור
1. מניעת גישה למידע	א. תוקף עשוי להצפין את המידע, ובכך למנוע גישה של מורשים אליו. ב. תוקף עשוי למחוק מידע ארגוני, לרבות גיבויים קיימים.
2. ערבול נתונים	תוקף עשוי לערבול נתונים, ובכך לפגוע במהימנות המידע. דוגמה לכך הינה שינוי סדר ההופעה או מיקום רשומות במסדי נתונים.
3. הדלפת מידע רגיש/חסוי	תוקף עשוי להדליף מידע רגיש/חסוי כשלב מקדים להפעלת הכופרה או במהלך הפעלתה.
4. סחיטה	א. תוקף עשוי לדרוש קבלת תמורה כלכלית או אחרת כתנאי לשחרור מפתח ההצפנה או הערבול. ב. סחיטה כפולה (Double Extortion) - תוקף עשוי לאיים בהפעלה של איום נוסף במקביל לכופרה

שם האיום	תיאור
	(דוגמת הפעלת תקיפת מניעת שירות מבוזרת) וזאת לשם הגברת עצימות הנזק.
	ג. סחיטה משולשת (Triple Extortion) - תוקף עשוי לפנות לגורמי צד-שלישי בדרישה לקבלת תמורה, וזאת תוך ציון כי אם לא יעשו כן, מידע רגיש/חסוי שלהם יודלף.
	ד. סחיטה הפוכה (Reverse Extortion) - תוקף עשוי להטמין בארגון "מידע מפלילי", ולהתנות אי- חשיפה / אי דיווח בקבלת תמורה.

טבלה 1: איומים עיקריים הנגזרים מתקיפת כופרה (Ransomware)

המציאות מלמדת כי ישנם מקרים בהם גורמים פנימיים (דוגמת אנשי סיסטם) הפעילו כופרה באופן יזום כנגד הארגון בו עבדו. לנוכח זאת, מומלץ כי הארגון יוודא כי ברשותו תוכנית מסודרת להתמודדות עם איום פנימי.



6. דרכי פעולה מומלצות - היערכות והתמודדות עם אירוע כופרה בארגון

פרק זה סוקר את דרכי הפעולה המומלצות לשם היערכות והתמודדות עם אירוע כופרה בארגון:

6.1 דרכי הפעולה המומלצות לשם היערכות לאירוע כופרה

תת-פרק זה סוקר רשימת פעולות מומלצות להיערכות אירוע כופרה:

מס'	הנושא	פירוט	גורם אחראי
כללי			
1.	מודיעין סייבר	האם הארגון מקבל מידע מודיעיני בנושא תקיפות כופרה? כיצד הארגון משתמש במידע זה לשם שיפור מערך ההגנה ותהליך ניהול הסיכונים? האם יש לארגון היכרות מקדימה עם אתרים מקובלים לקבלת מידע/תמיכה במקרה הצורך? לדוגמה The No More Ransom Project	צוות הגנה סייבר
2.	הסכמי שירות	האם ברשות הארגון הסכמי שירות אשר יוכלו לסייע במקרה של אירוע כופרה, והאם עוגנו בהסכם ההתקשרות מדדים רלוונטיים? כיצד נבחנת עמידת הספקים במדדים שהוגדרו? בכלל זה יש לתת את הדעת לסמכויות הארגון במקרה של אירוע סייבר	אגף מערכות המידע

	אשר מקורו בגורם משרשרת האספקה של הארגון.		
אגף מערכות מידע צוות הגנה סייבר	האם ברשות הארגון כ"א מתאים להיערכות והתמודדות עם אירוע כופרה על בסיס 24/7? אם לא, האם יש הסכם התקשרות מול ספק רלוונטי (דוגמת ספק המתמחה ב-DFIR ¹ או בשחזור מידע)?	הון אנושי	3.
המשכיות עסקית וגיבויים			
הנהלת הארגון	האם ישנו צוות ניהול משברים בארגון? אם לא, מי יהיה חבר בצוות? האם נדרש לבצע התקשרות עם גורם צד-שלישי שיוכל לסייע בעת הצורך? מי מוסמך לבצע אסקלציה ובאלו תנאים?	צוות ניהול משברים	4.
הנהלת הארגון	האם קיימת תכנית המשכיות עסקית? האם נושא הכופרה נכלל ברשימת התרחישים להתמודדות? האם ועדת היגוי דנה בתרחישים באופן עתי? האם תרחישי קיצון דוגמת מחיקה או אובדן של כלל המידע הארגוני זוכים להתייחסות? האם הוגדרו לכל	המשכיות עסקית	5.

¹ DFIR - Digital Forensics and Incident Response

	נכסי/תהליכי הליבה מדדים מקובלים (דוגמת RTO\RPO)? מה עושים עם שאר עובדי החברה בזמן משבר? האם שגרת העבודה נשמרת או נדרש לבצע שינוי בסדר היום?		
הנהלת הארגון	האם לארגון יש תכנית התאוששות מאסון? האם יש לארגון אתר חלופי? אם לא, מדוע? מתי האתר החלופי יופעל? כמה זמן ייקח להפעיל את האתר החלופי? האם האתר החלופי מבטיח עמידה במדדים אשר הוגדרו להמשכיות עסקית?	אתר חלופי (DR)	.6
אגף מערכות מידע	האם מערך הגיבוי חסין בפני תקיפות סייבר? כיצד נבחנת תקינות הגיבויים? האם מדיניות הגיבויים עונה לדרישות תכנית המשכיות עסקית? האם קיים הסכם התקשרות מול ספק שירות אשר יוכל לסייע במקרה של תקלה/בעיה בביצוע השחזור? להרחבה ראו "שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור"	גיבויים	.7
בדיקת מוכנות וכשירות			
צוות ניהול משברים	האם הארגון ביצע תרגול בשנה האחרונה של מערך	תרגול סייבר	.8

	<p>ההגנה תוך התייחסות לתרחישי כופרה מקובלים? אם כן, מה היו הממצאים? האם התרגול כלל ביצוע אסקלציה במקרה הצורך? האם המסקנות יושמו? האם שולבו גורמי צד-שלישי, דוגמת MSSP\MDR? האם תכנית התאוששות מאסון מכילה פרק תרגול ייעודי? האם ישנם נושאים נוספים שיש לתרגל?</p> <p>להרחבה ראו "תרגול בסייבר - בנייה ועריכה של תרגילי סייבר לארגון"</p>		
צוות הגנה סייבר	<p>האם הארגון יישם את בקורות ההגנה בתורת ההגנה בסייבר לארגון בגרסתה העדכנית? אם לא, מהו תאריך היעד? אלו משאבים יש להקצות על-מנת להשלים הטמעה אפקטיבית? האם ישנם חסמים שיש לטפל בהם לשם הצלחת התהליך?</p> <p>להרחבה ראו "טיוטה להתייחסות הציבור בנושא שיפורים ותוספות לתורת ההגנה"</p>	צמצום משטח תקיפה	.9
צוות הגנה סייבר	האם הארגון מבצע בדיקות חוסן עיתיות, תוך התייחסות לתרחישי תקיפה מסוג	בדיקות חוסן	.10

	כופרה?		
צוות הגנה בסייבר	האם הארגון מבצע סריקת פגיעויות / חולשות, תוך התייחסות ל-IOE's אשר שכיח כי כופרות מנצלות לרעה?	סריקת פגיעויות/חולשות	.11
צוות הגנה בסייבר	האם ברשות הארגון ניהול תגובה לאירוע בסייבר? האם הנוהל עדכני? מי אחראי לעדכן את הנוהל? האם הנוהל נכתב בהתאם למתודות עדכניות בתחום? האם קיים העתק מודפס של הנוהל כך שניתן להשתמש בו במקרה של העדר זמינות תשתית התקשוב?	נוהל תגובה לאירוע בסייבר	.12
צוות הגנה בסייבר	האם ברשות הארגון תהליכי בקרה רציפה ומתמשכת? אם לא, האם יש ברשות הארגון הסכם שירות מתאים מול MSSP\MDR? האם ישנם מדדים מתאימים לבחינת אפקטיביות?	בקרה רציפה (ומתמשכת Continuous Monitoring)	.13

טבלה 2: רשימת משימות מומלצות להיערכות אירוע כופרה

ככלל, צוות ניהול המשברים צריך לכלול את הנציגים הבאים לכל הפחות: מנכ"ל או משנה למנכ"ל, חבר הנהלה המייצג את הצד העסקי הפועל מול לקוחות, יועץ משפטי, מנהל מערכות מידע, ממונה הגנת מידע וסייבר/מנהל אבטחת מידע וסייבר, דוברות. כמו כן, יש לתת את הדעת למינוי גורם מחליף למקרה אי זמינות נציג מהרשימה לעיל.

6.2 דרכי הפעולה המומלצות לשם התמודדות עם אירוע כופרה

תת-פרק זה סוקר רשימת פעולות מומלצות להתמודדות עם אירוע כופרה:

מס'	הנושא	פירוט	גורם אחראי
זיהוי - ביצוע בירור ראשוני אודות היתכנות של אירוע סייבר, לרבות נקיטת דרכי פעולה מיידיות לטיפול.			
1.	ניטור סייבר	מיהו הגורם האחראי לגילוי וזיהוי הכופרה? מיהו הגורם האחראי לוודא כי אין מדובר בהתרעת שווא או תקלה תפעולית? מה אמינות מקור דיווח (המערכת או המכשיר המדווח)? האם קיים נוהל טיפול באירוע סייבר? מהם שלבי העבודה לפי הנוהל? מי אחראי לביצוע כל שלב? מיהו הגורם האחראי לתיעוד הפעילות המתבצעת במסגרת האירוע (ניהול יומן אירועים)? האם אותרו IOC's מוכרים או שישנה התנהגות/אנומליה חריגה המחייבת בחינה? האם בוצעו פעולות לשיפור איכות הניטור?	צוות הגנה סייבר
ניתוח - ביצוע בירור מקיף ומעמיק לגבי האירוע לשם אימוץ דפוסי פעולה הכרחיים תוך בחינת חלופות אפשריות לבלימה והתמודדות עם האירוע.			
2.	ממשל תאגידי	האם קיים תהליך לביצוע רכש מהיר במקרה הצורך?	אגף מערכות מידע רכש
3.		האם קיימת תוכנית	הנהלת הארגון

	<p>המשכיות עסקית (BCP)? מיהו האחראי להפעלתה ויישומה? מהם המדדים שהוגדרו לכל תהליך/נכס סייבר (RPO\RTO וכד')? מיהו הגורם המעדכן את צוות ניהול המשברים? מה קורה אם אותו גורם אינו זמין?</p>		.4
צוות ניהול משברים	<p>האם קיים נוהל טיפול במשבר? מהם שלבי העבודה לפי הנוהל?</p>		.5
אגף מערכות מידע	<p>האם הגיבויים תקינים? איך אנו יודעים שהגיבויים תקינים?</p>	בקרת נזקים ראשונית	.6
צוות הגנה סייבר	<p>אלו נכסי סייבר נפגעו? האם גורמי צד-שלישי נפגעו/יפגעו? האם מדובר במסך עשן (Fog Screen) להסתרת תקיפה אחרת? האם נוצלו לרעה IOE's מוכרים (בהתאם למודיעין סייבר וכד')? האם אותרו IOE's חדשים? האם ניתן להתחקות אחר אמצעי התשלום? מהו היקף ואיכות המידע שנפגע (CHD\CUI\PHI\PDI) וכד')? האם המידע הוצא על-ידי התוקף מחצרות/גבולות הארגון? האם ישנה דרישת תשלום? מי אחראי לוודוא כי הראיות נאספות ונשמרות בהתאם</p>		.7

	<p>לעקרון "שְׁרִשְׁרֵת מְשֻׁמֶרֶת" (Chain of Custody)? כיצד הוא מוודא זאת? לכמה זמן יש לשמור ראיות/מידע פורנזי, ומהו היקף השמירה (כל נכסי הסייבר, שרתים בלבד, נכסי סייבר שנפגעו בלבד, Image מלא? הגדרות תצורה בלבד? קבצים חשודים בלבד? וכד')?</p>		
צוות ניהול משברים	<p>מהו סוג הכופרה? מהן יכולות התקיפה שלה? מהי דרך החדירה? האם ניתן להסיר את הכופרה? מהי רמת הודאות שניתן לעשות את זה? האם מידע שדלף פורסם באינטרנט? רשתות חברתיות? Darknet? מהי המטרה של התוקף? כסף? פגיעה במוניטין? וכד' מיהו התוקף (בהנחה שניתן לזהותו)? האם ישנם פרסומים מחוץ לארגון אודות האירוע? כיצד מתמודדים עם פרסומים כוזבים (Disinformation)? האם לקוחות/ספקים וכד' פנו לארגון בתלונות? האם הוגשו תביעות נגד הארגון ו/או נושאי המשרה? האם הוגשו תלונות/קובלנות נגד הארגון ו/או נושאי המשרה? מה יקרה אם לא נשלם?</p>		.8

	מהי הדרך לקבלת פיצוי/שיפוי או שירות רלוונטי מחברת הביטוח?		
צוות ניהול משברים	בהינתן כי האירוע מקורו מגורם בשרשרת האספקה של הארגון, מי מוסמך לתקשר מולו? מהן חובות אותו גורם כלפי הארגון? האם ניתן לשלוח צוות DFIR מהארגון לאותו גורם?		.9
אגף מערכות מידע	האם חברי צוות הסיסטם הרלוונטיים זמינים ובעלי נגישות לנכסי הסייבר? האם נדרש לתגבר את צוות הסיסטם בגורמי צד-שלישי (דוגמת מומחה גיבויים)? אם כן, מהו ה-SLA?	כוח-אדם	.10
צוות ניהול משברים	האם על הארגון לתגבר את הצוות הקיים בגורמי מקצוע צד-שלישי? אם כן, האם יש לנו חוזה התקשרות עם גורמי מקצוע? מהו ה-SLA?		.11
צוות הגנה סייבר	האם ברשות הארגון צוות חקירה פורזנית ותגובה לאירועים (DFIR)? אם כן, מהו ה-OLA? אם לא, האם יש לנו חוזה התקשרות עם גורמי מקצוע חיצוניים? ואם לא, את מי נזמן? מהו ה-SLA?		.12
צוות ניהול משברים	האם ברשות הארגון ביטוח סייבר תקף? מיהי חברת הביטוח? מיהו סוכן הביטוח של הארגון? האם הביטוח הקיים מכסה	ביטוח סייבר	.13

	<p>סוגיות סייבר? אם כן, אלו תכולות שירותים הביטוח כולל? מהו ה SLA-ביחס לכל שירות? האם גורמי החוץ אשר הארגון מעוניין לזמן מוכרים ומורשים ע"י חברת הביטוח? האם עלינו לקבל את אישור חברת הביטוח לפני המשך פעולה? מהו היקף הפיצוי/השיפוי? האם זה משתלם לפנות לחברת הביטוח? מי הגורם בארגון המוסמך להתקשר עם חברת/סוכן הביטוח? האם הסוכן/חברת הביטוח זמינה להתייעצות בזמן זה? האם יש לנו איש קשר ספציפי בחברת הביטוח שזמין 24/7?</p>		
אגף מערכות מידע	<p>האם הגיבויים תקינים? איך אנו יודעים שהגיבויים תקינים? מהו הוא תאריך הגיבוי האחרון? כמה זמן ייקח לשחזר את הנכס/המידע? כמה מידע/זמן עבודה נאבד לאחר שחזור המידע? מהו סדר השחזור? על סמך מה הסדר נקבע? מה יעשה אם העתק הגיבוי יתגלה כתקול או כנגוע? האם ניתן לעשות שימוש ביכולת המובנית במערך</p>	בדיקת הגיבויים	.14

	<p>האחסון/הסביבה הווירטואלית לחזרה ל"תמונת מצב" (Snapshot) מוגדרת? האם ניתן להביא מערכת גיבוי נוספת לקיצור זמן השחזור? האם ברשות צוות הסיסטם רישוי, Images ותוכנות ממקור מהימן אשר יאפשרו ביצוע שחזור או התקנה מאפס בעת הצורך? האם פעולת השחזור תשמיד ראיות נדרשות, ואם כן, אלו צעדים נדרשים לביצוע לשם הגנה עליהן?</p>		
צוות הגנה סייבר	<p>האם הגיבויים שברשות הארגון אינם מכילים נוזקות? כיצד נוכל להבטיח שהמידע המשוחזר אינו מכיל נוזקות?</p>		.15
אגף מערכות מידע	<p>מהי רמת המוכנות והכשירות של אתר ה-DR?</p>	אתר DR	.16
צוות ניהול משברים	<p>האם ישנו צורך לדלג לאתר DR? מהי הסבירות להצלחה של מעבר בהתאם למדדים שהוגדרו?</p>		.17
הכלה - השגת שליטה ראשונית של האירוע לצורך הכלתו ועצירת החמרת השפעתו על פעילות הארגון.			
צוות הגנה סייבר	<p>האם נדרש לנתק את הקישור לממשקים חיצוניים דוגמת האינטרנט? מהן ההשלכות האפשריות מכך? מי מוסמך לאשר ביצוע? האם נדרש לנתק את</p>	צמצום אפקט הנזק	.18

הקישור לממשקים פנימיים
דוגמת הקישור לאתר DR ?
מהן ההשלכות האפשריות
מכך? מי מוסמך לאשר
ביצוע?
האם נדרש לנתק את מערך
הגיבוי / האחסון מהרשת?
מהן ההשלכות האפשריות
מכך? מי מוסמך לאשר
ביצוע?
האם נכסי סייבר שנפגעו
נותקו מהרשת? אם לא,
מדוע?
האם נדרש לבצע פעולות
נוספות לצמצום משטח
התקיפה/הגבהת חומות?
האם מדובר בנוזקה מוכרת?
האם ישנן דרכים לחלץ את
המפתח? האם השימוש
במפתח מאפשר שחזור של
המידע?
האם יש ברשות הארגון
תיעוד (לוגים, קבצי
היסטוריה, אחר)
וארטיפקטים (Artifacts)
אחרים אשר יוכלו לסייע
בחקירה?
האם ברשות הארגון כלים
מתאימים לביצוע החקירה?
האם ישנם סממנים לרמת
המורכבות (דוגמת יכולת
חמקנות) של הנוזקה?
כמה זמן מתקיימת אחיזת
תוקף?

צוות ניהול משברים	<p>מיהם בעלי העניין החייבים בדיווח? לקוחות? ספקים? רגולטורים? מהו ערוץ הדיווח (מייל? טלפון? וכו')? האם יש צורך לעשות שימוש ב-TLP בעת העברת מידע?</p> <p>האם נדרש לוודא הגעה של הדיווח/ההודעה? מה חלון הזמן לדיווח? האם יש מקרים בהם נדרש לעדכן אודות התפתחות האירוע גם לאחר הדיווח הראשוני? מהו הטריגר להמשך דיווח ומיהו הגורם המורשה להעביר דיווח?</p> <p>האם מערך הסייבר הלאומי עודכן על אודות האירוע? אם לא, מדוע?</p>	חובת דיווח	.19
צוות ניהול משברים	<p>האם הארגון ישוחח עם גופי התקשורת? האם יש ברשות הארגון נוסח מוכן ("תבניות") של הודעות לפרסום? מיהו הגורם המוסמך לדבר על כך בתקשורת? האם עובדי הארגון תודרכו בנושא הרגישות של הנושא/מותר ואסור להם בנושא והאם המעגל המטפל באירוע תודרך בהתאם מבחינת מסרים וכו'?</p> <p>האם הוגדר תהליך שקיפות מול לקוחות וספקים אודות המצב? מידע אודות מה</p>	ממשקי תקשורת פנימיים/חיצוניים	.20

	<p>קרה, מה הנזק המוערך, מהן ההמלצות לספקים/לקוחות שפרטיהם נמצאים בסכנה? מה מומלץ להם לבצע? כיצד אתם מתמודדים עם האירוע ומה עתיד לקרות? טלפון/מייל ליצירת קשר? האם יש פרסומים אודות האירוע בערוצי התקשורת? האם יש פרסומים אודות האירוע ברשתות החברתיות? האם ישנה השפעה על ערך המנייה? פניות משקיעים? פניות מגורמים אחרים?</p>		
צוות ניהול משברים	<p>מי מנהל את המשא ומתן? מהן מטרות הארגון במשא ומתן (משיכת זמן)? מי מפקח אחר ביצוע הפעילות? מהי מטרת התוקף? האם ניתן למשוך זמן עד להשלמת פעולות החירום? האם ישנן דרישות מיוחדות מצד התוקף? האם התוקף חשף מידע ייחודי? מה יעשה אם לא ניתן לשחזר את המידע? האם התקבלו הנחיות ספציפיות מרגולטור או גורם אחר?</p>	ניהול משא ומתן	21.
הכרעה - נטרול רכיבי התקיפה שמצויים במערכות הארגון תוך שאיפה למזעור הנזק שנגרם בשל המתקפה.			
צוות הגנה סייבר	<p>האם הנוזקה הוסרה? האם כל נכסי הסייבר נקיים? מה</p>	הסרת הנוזקה	22.

	<p>ימנע הדבקה חוזרת של נכסי הסייבר? האם ישנם מזהים שניתן לכייל (IOC's\IOA's) במערך האבטחה? האם ישנן הנחיות מסודרות להסרת הנוזקה? כיצד ניתן לדעת שהנוזקה הוסרה, ושאינן נזקות נוספות שיש להן אחיזה בתשתית ומערכות הארגון?</p>		
צוות ניהול משברים	<p>מיהו הגורם האחראי למעקב/בקרה אחר ביצוע הפעולות הנדרשות? מה יעשה אם לא ניתן לשחזר את המידע? האם התקבלו הנחיות ספציפיות מרגולטור או גורם אחר?</p>		.23
אגף מערכות מידע	<p>האם צוות הסיסטם יודע מה עליו לעשות על-מנת להסיר את הנוזקה? האם צוות הסיסטם צריך לבצע התקנה מחדש של מערכות הפעלה מאפס? האם צוות הסיסטם צריך לבצע הסרה של הנוזקה ע"י סקריפטים או שיטה אחרת? האם יש צורך לגבות מידע שהוצפן, כך שניתן יהיה לשחזר אותו בעתיד במקרה של חשיפת מפתח?</p>		.24
	<p>האם וכיצד ניתן להסיר מידע שדלף לאינטרנט, Darknet, רשתות חברתיות?</p>	הסרת מידע שדלף	.25

צוות ניהול משברים	מהם הנזקים אשר נגרמו עד כה לארגון? מהן ההשפעות בטווח הקצר והארוך? האם ניתן לצמצם את הנזקים? מה קורה אם מתגלה שהאירוע לא הסתיים ואולי אף מוחרף?	בקרת נזקים	.26
השבה - חזרה לתקינות ופעילות מלאה של הארגון המותקף.			
אגף מערכות מידע	האם קצב ואיכות שחזור עומדים במדדים הנדרשים? אם לא, מה אפשרי לעשות על-מנת לשפר את המצב? האם פעולות השחזור הסתיימו באופן מוצלח מבחינת צוות הסיסטם?	ביצוע שחזור של מידע	.27
צוות הגנה סייבר	האם הסביבה אליה המידע ישוחזר נקיה מנוזקות? האם/כיצד ומי אחראי לבדיקה שלא קיימת אחיזה של התוקף ברשת הארגונית לצורך הדבקה חוזרת והסלמת האירוע? האם אין סממנים (IOA's\IOC's\TTP's) שהאירוע חוזר על עצמו?		.28
צוות ניהול משברים	מיהם הגורמים העסקיים שבדקים שתהליך השחזור פעל כמצופה, וכי הנכסים שמישים לעבודה?		.29
צוות ניהול משברים	האם ישנה כדאיות כלכלית לבקש פיצוי/שיפוי מחברת הביטוח? כיצד ניתן לקבל פיצוי/שיפוי מחברת הביטוח בגין הנזקים שנגרמו? מה עושים אם חברת הביטוח מסרבת	ביטוח סייבר	.30

	לשלם?		
צוות ניהול משברים	האם מתבצעים תהליכים מקובלים לחזרה לשגרה מפוקחת (תקופה בה מתבצעות פעולות מוגברות לגילוי וזיהוי תוקף)? כמה זמן היא תיקח (75 ימים כמינימום מומלץ)? מה קורה אם מתגלה שהאירוע לא הסתיים ואולי אף מוחרף?	חזרה לשגרה מפוקחת	.31
צוות הגנה סייבר	האם ניהול התחקיר מבוצע ע"י גורם בלתי תלוי נטול השפעה פנימית? מהם הכשלים במערך האבטחה שאפשרו את הצלחת התקיפה? מה נדרש לשפר במערך האבטחה? מי אחראי לשיפור מערך האבטחה? כיצד ניתן לוודא את אפקטיביות בקורות ההגנה, וזאת למניעת הישנות האירוע? מתי ומי אחראי לביצוע תרגיל סייבר לבחינת מוכנות וכשירות הארגון?	ניהול תחקיר והסקת מסקנות	.32
צוות ניהול משברים	מתי ומי מנהל את התחקיר? מהם ממצאי התחקיר? מה נדרש לבצע על-מנת למנוע הישנות של האירוע? מי אחראי ליישם את המלצות התחקיר? כיצד הארגון מאמת כי המלצות התחקיר יושמו		.33

	<p>באופן אפקטיבי? מיהו הגורם האחראי להקצאת משאבים לתוכנית שדרוג/שיפור תשתיות המחשוב? האם צריך לשלוח את ממצאי התחקיר לרגולטור או לגורם אחר? האם נדרש לפרסם את הממצאים בדו"חות ציבוריים (דוגמת דיווח לבעלי מניות), ואם כן איזה מידע נדרש, וכיצד נמנע חשיפת מידע רגיש/חסוי שלא לצורך?</p>		
צוות ניהול משברים	<p>אלו פעולות נדרש לבצע לשם שיקום מוניטין הארגון (החזרת אמון הלקוחות והמשקיעים)? מי אחראי לבצע זאת? מהם המשאבים הנדרשים? כיצד ניתן להבטיח בסיום הפעילות כי פעולות השיקום צלחו?</p>	שיקום מוניטין	.34
צוות ניהול משברים	<p>מתי מכריזים על חזרה לשגרה רגילה? האם ישנן סנקציות רגולטוריות נגד הארגון או נושאי המשרה? מי מטפל בהן? האם ישנן תביעות נגד הארגון או נושאי המשרה? מי מטפל בהן?</p>	חזרה לשגרה רגילה	.35

טבלה 3: רשימת משימות מומלצות להתמודדות עם אירוע כופרה

7. נספחים

פרק זה מכיל את רשימת הנספחים הנלווים למסמך זה.

נספח 1 - דרכי התמודדות מומלצות - היערכות והתמודדות עם אירוע כופרה (Ransomware) בארגון

מטרת הנספח

לשקף לקורא את אופן פיתוח המסמך, הגורמים המעורבים בתהליך כתיבתו ובהעברת משוב על התכנים לטובת מתן שקיפות וגילוי נאות לתהליך ולגורמים המעורבים על סוגיהם.

א. כיצד גובש המסמך - סקר שוק/סילבוס/השוואה בעולם

- 1) בחינה של תיעוד/תקינה מהעולם כגון NIST, ISO, ועוד (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
- 2) בחינה של פרסומים מקובלים בתחום (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
- 3) קבלת משוב מהציבור לטיוטות המסמך אשר פורסמו:
 - א. מר מריו ליכטמן
 - ב. עו"ד ורד זליכה

8. קיצורי שמות

פרק מציג את קיצורי השמות בהם נעשה במסמך זה.

שם המונח	ביאור
BCP	Business Continuity Planning
CHD	Cardholder Data
CISO	Chief Information Security Officer
CUI	Controlled Unclassified Information
DDoS	Distributed Denial-of-Service Attack
DFIR	Digital Forensics and Incident Response
DR	Disaster Recovery

שם המונח	ביאור
IOA	Indicator of Attack
IOC	Indicator of Compromise
IOE	Indicator of Exposure
MDR	Managed Detection and Response
MSSP	Managed Security Service Provider
OLA	Organization Level Agreement
PHI	Protected Health Information
PII	Personally Identifiable Information
RaaS	Ransomware as a Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
TLP	Traffic Light Protocol
TTP	Tactics, Techniques, and Procedures

טבלה 4: קיצורי השמות בהם נעשה שימוש במסמך זה

9. מסמכים ישימים

פרק זה מכיל את מקורות המידע עליהם הסתמכו הכותבים בעת כתיבת המסמך.

מקורות מידע בעברית:

מערך הסייבר הלאומי

תרגול בסייבר - בנייה ועריכה של תרגילי סייבר לארגון

✓ <https://www.gov.il/he/departments/general/cyberexercise>

שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור

✓ https://www.gov.il/he/departments/general/backup_restore

התמודדות ארגונית במרחב הסייבר עם האיום הפנימי

- ✓ https://www.gov.il/he/departments/general/coping_thret

חיזוק זיהוי משתמשים במערכות ותשתיות של ארגונים ע"י שימוש באימות רב-גורמי (MFA)

- ✓ <https://www.gov.il/he/departments/general/mfa>

תורת ההגנה בסייבר לארגון

- ✓ https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר

- ✓ <https://www.gov.il/he/Departments/news/cybercrisispreparedness>

שאלון ספקים לחיזוק שרשרת האספקה

- ✓ <https://www.gov.il/he/departments/news/queriesupply>

שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור

- ✓ https://www.gov.il/he/departments/general/backup_restore

חקיקה

תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017

חוק הגנת הפרטיות, תשמ"א-1981

חוק חתימה אלקטרונית תשס"א-2001

חוק הארכיונים, תשט"ו-1955

חוק איסור הלבנת הון, תש"ס-2000

General Data Protection Regulation (GDPR)

רגולציה

דיווח על אירועי כשל טכנולוגי ואירועי סייבר, נב"ת 366, בנק ישראל

- ✓ <https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/Pages/nihultakin.aspx>

טופס דיווח על אירוע אבטחה חמור, רשות הגנת הפרטיות

- ✓ <https://formspdf.justice.gov.il/PrivacyProtectionAuthority/ReportingSecurityIncident.aspx>

עמדה משפטית מספר 33-105: גילוי בנושא סייבר, רשות לניירות ערך

- ✓ https://www.isa.gov.il/%D7%92%D7%95%D7%A4%D7%99%D7%9D%20%D7%9E%D7%A4%D7%95%D7%A7%D7%97%D7%99%D7%9D/Corporations/Staf_Positions/SLB_Decision/Reports/Documents/SLB_105-33_cyber.pdf#search=%D7%A1%D7%99%D7%99%D7%91%D7%A8

רענון חובות הגילוי במקרה של אירוע סייבר בהתאם לעמדת סגל 33-105 - גילוי בנושא סייבר, רשות לניירות ערך

- ✓ https://www.isa.gov.il/%D7%92%D7%95%D7%A4%D7%99%D7%9D%20%D7%9E%D7%A4%D7%95%D7%A7%D7%97%D7%99%D7%9D/Corporations/Hodaot_segaL/General/Documents/HODAA211220.pdf#search=%D7%93%D7%99%D7%95%D7%95%D7%97%20%D7%90%D7%99%D7%A8%D7%95%D7%A2

מדריך סייבר: עמידה בתנאים של היתר רעלים בתחום הסייבר בתעשייה, משרד הגנת הסביבה

- ✓ https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

כללי

מקורות מידע באנגלית:

General

The No More Ransom Project

- ✓ <https://www.nomoreransom.org/he/index.html>

TECHNICAL GUIDELINE ON INCIDENT REPORTING UNDER THE EEC, ENISA

- ✓ <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc>

RTF Report: Combatting Ransomware, IST Institute

- ✓ <https://securityandtechnology.org/ransomwaretaskforce/report/>

Regulation

PCI Standard

NIST

SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

- ✓ <https://csrc.nist.gov/publications/detail/sp/800-137/final>

Draft SP 800-137A - Assessing Information Security Continuous Monitoring (ISCM) Program

- ✓ <https://www.nist.gov/news-events/news/2020/01/assessing-information-security-continuous-monitoring-iscm-programs-nist>

*** סוף מסמך ***