מועצה אזורית מטה יהודה בלב המדינה

נוסח הודעה מורחבת למשתמשים

חובת יידוע משתמשים בעניין ניטורי סייבר ואבטחת מידע ברשת המחשוב המשרדית

איזה מידע נאסף באמצעות מערכות האבטחה?	המידע שנאסף הוא מידע שנוצר באופן שגרתי במסגרת פעילותה השוטפת של הרשת והמחשב. מהמידע ומניתוחו ניתן ללמוד על השימוש במערכות, כלומר מידע על תקשורות ופעילויות שונות הקשורות בהפעלת המחשב, לרבות גלישה באינטרנט ושליחת דואר אלקטרוני. רוב מוחלט של המידע שנאסף הוא מידע על אודות אופן פעולת המערכות, שידוע כ – "מידע על המידע". אגב איסוף מידע זה נאספים גם רכיבי מידע על השימוש של העובדים ברשת המכילים גם חלקים מתוכן המידע עצמו , כדוגמת נתונים על גלישה באינטרנט ותוכן תעבורת דואר אלקטרוני בתיבה המשרדית. על מידע זה נעשים עיבודים כדי לחלץ "מידע בעל ערך אבטחתי" – כלומר מידע שעשוי ללמד על "תקיפת סייבר" או ניסיון לתקיפת סייבר במשרד. "תקיפת סייבר" היא למעשה קובץ תקיפה זדוני הפועל ברשתות המשרד , ועל מנת לאתרו נדרש למצוא סימנים לפעילותו או לתקשורת שלו עם מפעיליו. דוגמא למידע על פעילות חריגה של ניסיונות של מחשב ליצור (log files) כזה הוא תיעוד בקבצי-יומן קשר עם אתר אינטרנט חשוד, שעשויה ללמד על ניסיונות תקיפה.
תדירות האיסוף	המידע נאסף באופן שוטף כל הזמן.
למה נאסף המידע?	איסוף המידע נעשה לצורך ניתוחו, עיבודו והצלבתו עם דפוסי תקיפה או מידע מודיעיני (מסחרי ואחר) על שיטות תקיפה ודרכי תקיפה, לצרכי הגנת הסייבר. בנוסף, איסוף המידע מאפשר איתור מוקדם של תקיפות על הרשת המשרדית והממשלתית, באמצעות הצלבת מידע ממקורות שונים בתוך המשרד ובין משרדי הממשלה ורשויות מקומיות וגופים ציבוריים. זאת, בדומה למתרחש כעת בתחום שיתוף המידע על עומסי תנועה בכבישים, על בסיס הבנה שהשלם גדול מחלקיו. המידע שנאסף במערכות לא מיועד ולא אמור לשמש למעקב אחר עובדים, אלא לצורכי הגנת הסייבר. המידע ינותח, יעובד ויופק ממנו מידע בעל ערך אבטחתי לאיתור תקיפות סייבר ולשמירה על מערכות המשרד והממשלה. כמו כן, יועברו התראות למשק על תקיפות סייבר בהתבסס על המידע האמור. במרבית המקרים, לא יכילו התראות כאמור מידע פרטי מתוך המידע שנאסף. אולם בנסיבות חריגות תתכן העברת מידע פרטי במסגרת ההתראות למשק. זאת, רק כאשר הדבר נדרש בדחיפות לשם התמודדות עם אירוע סייבר , ובנסיבות העניין, בשים לב לרגישות המידע ולחומרת האירוע, לא יהיה בשימוש במידע משום הפרה של הוראות חוק הגנת הפרטיות או כל דין אחר. לעניין זה ראו עקרונות הפעולה של המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר שאושרו על ידי היועץ המשפטי לממשלה https://www.gov.il/BlobFolder/policy/principles/he/principles.pdf במידע פרטי שנאסף לא ייעשה שימוש לכל תכלית אחרת, לרבות לשם פיקוח, אכיפה ומשמעת, למעט אם מסירת המידע מחויבת על פי דין.
מי אוסף את המידע ומי חשוף אליו?	המידע נאסף במסגרת פעילות ההגנה והתפעול השוטפת במשרד וביחידת ממשל זמין (מערך הדיגיטל) במסגרת ההפעלה של מערכות התקשוב הממשלתיות והציבוריות לרבות ברשויות המקומיות. כמו כן, נאסף המידע במערכות מרכזיות ביחידה להגנת הסייבר שברשות התקשוב הממשלתי, ובמערך הסייבר הלאומי (גופי ההגנה) , המפעילים את מרכז השליטה והבקרה הממשלתי למול איומי סייבר (ה-הממשלתי והציבורי ובשלטון המקומי). https://www.gov.il/he/departments/israel_national_cyber_directorate/govil-landing-page https://www.gov.il/he/departments/units/yahavsoc/govil-landing-page כאמור, המידע נאסף **לצורכי הגנת הסייבר**, ובמסגרת זאת נועד להתריע מפני תקיפות סייבר או פוגעני סייבר, לסייע בטיפול באיומי סייבר ולהפיץ מידע על דרכי התגוננות. רוב מוחלט של המידע נאסף ומנוטר באופן אוטומטי בלבד. תעבורה שעולה חשד כי היא קשורה לתקיפת סייבר עשויה להיבדק גם על ידי בעלי תפקידים בתחום הגנת הסייבר בגופי ההגנה, ובמסגרת בדיקה זו ייתכן שיחשפו גם לחלק מתוכן המידע.
ניטור תעבורה מוצפנת	חלק מאתרי האינטרנט מצפינים באופן שגרתי את תעבורת האינטרנט בינם לבין מחשב הגולש. לשם ניטור תעבורה זו, חלק ממערכות אבטחת המידע יפענחו באופן אוטומטי את ההצפנה, ולאחר ניטור התעבורה יצפינו אותה מחדש.

מה מתחייבות היחידה להגנת הסייבר ומערך הסייבר הלאומי בקשר למידע?	גופי ההגנה מודעים לכך שהמידע יכול להיות מידע בעל רגישות מטעמים שונים. בהתאם, גופי ההגנה נערכים לוודא כי נעשים כל הצעדים הנדרשים כדי לשמור על זכויות העובדים והם פועלים בהתאם לעקרונות שאושרו בידי היועץ המשפטי לממשלה– שמטרתם מיקוד בטיפול במידע המאפשר טיפול בתקיפה. לכן, גופי ההגנה מתחייבים: • להשתדל להפוך את המידע שמתקבל ב SOC הממשלתי למידע שלא ניתן לזיהוי, ככל שניתן תוך שימוש בכלים מקובלים. • לעבד את המידע לשם איתור והפקה של מידע בעל ערך אבטחתי, ופעולות נדרשות לצורך הגנת הסייבר. • לאבטח את המידע בהתאם לכללים וסטנדרטים מחמירים. • לשמור את המידע לפרק הזמן המינימאלי הנדרש לצורכי הגנת הסייבר בלבד. • להשתמש במידע שנאסף לצורכי הגנת הסייבר ויישום מדיניות הגנת הסייבר הממשלתית בלבד, ולא לשום מטרה אחרת, למעט אם מסירתו נדרשת על פי דין • לאפשר לכל עובד לעיין במידע על אודותיו במערכות, ככל שניתן באופן סביר • לזהות את המידע האמור ; יודגש כי המידע שנאסף במערכות מבוסס על מידע במערכות המשרדיות , ולכן לשם קבלת תמונה מלאה יותר על המידע אודות העובד מומלץ לפנות בבקשת עיון קודם כל אל המשרד המעסיק.
האם יש לי אפשרות לשלוט בהיקף המידע הפרטי שלי שנאסף במערכת?	כאמור , כלל הפעילויות ברשת המשרדית מנוטרות באופן אוטומטי , ובמקרה של חשד לתקיפת סייבר, נדרש לברר האם אכן מדובר בתקיפה, וככל שכן לטפל בה. הסיכון כי בעת הניטור יהיה צורך בצפייה בנתונים אישיים, מתרחש במקרים בהם ישנו חשד לתקיפה, וזו יכולה לצמוח מפעילות יזומה של העובד , בין מקצועית ובין פרטית או מתקיפת סייבר מגורם חוץ המופנית אל העובד. לכן , אין אפשרות לנטר באופן שונה פעילות פרטית ופעילות לצרכי העבודה במרחב הרשת. לצד האמור, לכל עובד יש אפשרות לבצע גלישה ממכשירו הסלולרי או מאמצעי טכנולוגי פרטי שהוא מביא עימו למקום העבודה ושאינו מחובר לרשת המשרדית. על כן, במקרים בהם חשוב לעובד שלא ליטול שום סיכון לפגיעה בפרטיות, אף לא סיכון שהסתברותו נמוכה, עומדת לעובד האפשרות לבצע את הפעילות הפרטית הנחוצה מן המכשיר הפרטי.
למידע נוסף	privacy@cert.gov.il