



תכנית המשכיות עסקית - הדרך לצליחת משבר סייבר

אירועי תקיפות סייבר חוזרים ונשנים בשנתיים האחרונות על בתי עסק מוכיחים שוב ושוב את חשיבותה של היערכות נכונה - הן טכנולוגית, הן מנהלתית

וחוסן לאומי בסייבר, מערך הסייבר הלאומי מקדם את נושא ההיערכות בסייבר למצבי משבר. מרכיב מהותי בהיערכות זו הוא 'התפיסה הלאומית בסייבר להיערכות ולניהול מצבי משבר'."

היטיב לתאר את המצב ראש מערך הסייבר כשבריאיון ל"ידיעות אחרונות" מתאריך 14.1.22 אמר:

"מאז 24 באפריל 2020, היום שבו טהרן תקפה משאבות מים ברחבי ישראל, אנחנו במצב מלחמה. וזה שאתם לא שומעים כדורים שורקים מעל הראש, ממש לא אומר שאין נפגעים."

על מנת להיערך למלחמה הזו, שעלולה בכל רגע לפלוש לארגון שאותו אתם מנהלים ולהשפיע ישירות על המידע שנאסף ונשמר ואשר עליו אתם אחראים, אין מנוס מלהכין תכנית הגנה. בתכנית זו נעוץ המפתח לצליחת אירוע סייבר בטר"ש או צל"ש."

התרחישים ידועים. חובת ההנהלה להיערך בהתאם

משבר סייבר פוגע טכנולוגית ויוצר הפרעה עסקית היקפית ניכרת שממשיכה לייצר גלי הדף גם לאחר סיומו של המשבר. היערכות נכונה היא בין היתר תכנית טובה שתעסוק בשילוב יכולות ידניות, כל עוד המכונה הטכנולוגית מושבתת, לצד התמודדות תקשורתית נכונה, הן פנים ארגונית, הן כלפי חוץ - ללקוחות, שותפים עסקיים ותקשורת.

מנכ"ל שמשוחח עם התקשורת בעיצומו של משבר סייבר ואומר דברים לא נכונים, עלול לגרום לטעות עסקית שבתום המשבר יהיה קשר מאוד לתקן. מקרה כזה הוא דוגמה לחוסר מוכנות.

עסק שאינו מתרגל תקופתית את בדיקת הגיבויים, איכותם ומשך הורדתם, פוגע במוכנות המשכיות עסקית בעת משבר, ללא פגיעה בפריץ.

ארגון שאינו ערוך עם רשימת טלפונים למומחים שיסייעו לו להתמודד עם האירוע מבעוד מועד הוא ארגון שאינו מוכן לתקיפת סייבר.

הנהלה שלא תרגלה אירוע 'על יבש', לרבות תרגול תכנית המשכיות עצמה, תמצא את עצמה ללא כלים ניהוליים נאותים לצלוח משבר ללא נזקים ישירים ועקיפים.

תכנית המשכיות עסקית טובה תכלול ניהול של

בין אם היו אלה אירועי הטרור ב-11 בספטמבר 2001 אשר העלו את הנושא לראשונה, ובין אם הייתה זו מלחמת המפרץ עשור קודם לכן שעשתה זאת - אין כיום כל מחלוקת באשר למודעות לצורך של ארגונים להשקיע בהיערכות להתאוששות מאסון באופן שיאפשר המשכיות עסקית. בשנתיים האחרונות, בצל מתקפות הסייבר התכופות והמתוחכמות שאנו חוזים בהן, המשכיות עסקית נהייתה חיונית עוד יותר.

כדאי להבין ש"תכנית המשכיות עסקית" Business Continuity Plan (BCP) או "תכנית התאוששות מאסון" Disaster Recovery Plan (DRP) היא חלק בלתי נפרד ממוכנות נכונה למשבר סייבר בעסק שלכם.

מלבד רגולציית אבטחת המידע הקיימת, כגון תקנות הגנת הפרטיות (אבטחת מידע) 2017, המבוססות על חוק הגנת הפרטיות 1981, וגילויי דעת של רשם מאגרי המידע ברשות להגנת הפרטיות, המהווים גם הם רגולציה לכל דבר ועניין, בימים אלה שוקדים באגף הפיקוח על הביטוח ברשות שוק ההון, ביטוח וחסכון, על רגולציה סקטוריאלית המיועדת לסוכנים ולסוכנויות הביטוח בישראל.

אך המלצות הרגולטור למניעת אירוע או הקטנת הסיכון להתרחשותו, אינן בהכרח מבטיחות מוכנות לאירוע.

המפתח לצליחת משבר סייבר ללא נזק או עם נזק מינימלי טמון בהיערכות נכונה. היערכות משמעה מוכנות ותרגול. זו גם התפיסה הלאומית בסייבר להיערכות והתמודדות עם מצבי משבר - תפיסה המבוססת בפרסומים והמלצות של מערך הסייבר הלאומי, המיועדים למרחב הסייבר הציבורי, או, כפי שהובא בתקציר המנהלים של המערך למסמך התפיסה הלאומית:

"העלייה ביכולות התוקפים ובמאמציהם במרחב הסייבר, בד בבד עם התלות הגוברת במערכות מחשוב, מגדילות מאוד את הסבירות להתרחשות משבר סייבר רחב ומתמשך, בעל פוטנציאל נזק אדיר לארגונים, למגזרים עסקיים ואף למדינות. על מנת להתמודד עם משבר סייבר ביעילות, נדרש לבצע היערכות מקדימה, שתאפשר לנהל את המשבר באופן שיקטין את נזקיו והשלכותיו ויקצר את משכו. לפיכך, במסגרת פעולותיו לבניית עמידות





למקצוענים בביטוח

מנוי עדיף

שומר אותך
מעודכן ומקצועי
בכל מקום ובכל זמן

מוסיפים לך ערך

עדיף עכשיו

שירות מבזקים בנושאים ותחומים על פי בחירה

הנחות והטבות על כל מוצרי עדיף

איתור מידע מקצועי

דוחות, חוזרים והנחיות, פסקי דין ועוד...

עדיף WhatsApp

קבלת מידע מקצועי ועדכונים חשובים בזמן אמת

ניוזלטר יומי

מרכז את אירועי היום

שבועון עדיף

מרחיב ומעמיק נושאים אשר על סדר היום

מרכז מומחים משיבים

מוסחים עונים על שאלות מקצועיות שלכם

עדיף TV

מתחם תוכן המרכז שידורי לייב, תכני וידאו ופודקאסטים

גישה לפורטל עדיף

לפרטים נוספים 03-9076000
info@anet.co.il

תהליכים בעת משבר בכל אחת מהגזרות בארגון: כוח אדם, משפטי, טכנולוגי, יח"צ ומוניטין, שרשרת אספקה, נהלים, תרגולים, תרחישי סיכון, ממצאים ומשימות.

גל מתקפות מתוחכמות אך לא מאוד מורכבות מבחינת טכנולוגית שטף אותנו בשנתיים האחרונות. ואף שהמתקפות לא היו מתוחכמות במיוחד, הן גרמו נזק אדיר והציגו כישלון בניהול המשבר. מדוע? כי היה צריך ואפשר להיערך אחרת. היערכות נכונה הייתה מציגה תוצאה שונה בתכלית.

בית חולים הלל יפה לדוגמה, הוא יעד מועדף לתקיפות, בדיוק כמו כל בית חולים אחר בארץ או בעולם. הוא יעד מועדף מכיוון שמערכות של בית חולים כוללות עשרות ישומונים המאפשרים תקיפה קלילה שתשאיר אחריה נזק גדול. כאשר התוקף מצפין את הנתונים ומשבש אותם, בית החולים ניצב בפני מצב שבו כל התהליכים הרפואיים נעצרים ועוברים להתנהל בנייר ועיפרון. מד"א מפסיקה לפנות חולים, התקשורת מעצימה את האירוע ובית החולים הושבת למשך חודשיים, שבהן תועדו הפעולות בקלסרים.

האם היה אפשר להיערך אחרת? ודאי שכן, ולא רק בהקשר הטכנולוגי, שמשמעו בעיקר ביצוע גיבויים באמצעות גורמים חיצוניים שאי אפשר לשבשם או לזהמם. אך החשוב יותר הוא היערכות בפן הניהולי. היכולת לתפקד מבלי לשבש תהליכים בארגון באמצעות נייר ועיפרון. ושוב, בתי חולים רבים מותקפים כל העת, אך צולחים את האירוע ללא פגיעות חמורות כי הם נערכו כנדרש לתרחישי סיכון מעבר לסיכון הטכנולוגי המובהק.

מבית החולים כמשל נחזור בחזרה לענף הביטוח: האם אתם ערוכים למתן שירות סדיר באמצעות נייר ועיפרון או טופס הצעה, כאשר מכונת הטכנולוגיה כולה מושבתת?

המפתח הוא בהיערכות להמשכיות עסקית, ובתכנית שתכלול את רשימת איומי הייחוס לארגון שאותו אתם מנהלים, היערכות טכנולוגית, היערכות פרוצדורלית (כגון: צוות מענה לתוקף, צוות משפטי, דוברות) והיערכות לרציפות עסקית תוך כדי אירוע.

ואם הגעתם עד כאן ואתם עדיין סבורים שמתקפת סייבר יכולה להסתיים בפירמוט מחשבים והורדה מגיבויים, כדאי לזכור שעל פי הרגולציה, התעלמות מאירוע ללא בדיקה אם דלף מידע מהארגון מהווה עבירה על החוק - וזהו סיכון נוסף שיש לנהל.

הכותבת מלווה חברות וארגונים במגזר הפיננסי, בהטמעת תהליכי הגנה על המידע - as a Service DPO ושותפה עם משרד עו"ד קן-דרור הראל ושות' - בתחום הגנת המידע