

תקלת CrowdStrike - ניהול סיכונים במערך טכנולוגיית המידע בארגון עדכון לקוחות - יולי 2024

לקוחות יקרים,

ביום שישי ה-19 ביולי 2024 ארעה תקלת מחשוב שמקורה בחברת CrowdStrike, חברה גלובאלית שמתמחה באבטחת סייבר, בהגנה על ארגונים מפני איומים מתקדמים ופריצות לרשתות.

מבוקר אותו היום, הגיעו דיווחים בדבר בעיה חמורה שמשפיעה על מערכות Windows שמריצות את תוכנת Falcon של החברה. עוד דווח כי מערכת ההפעלה Windows קרסה ומשתמשים נתקלו במסך כחול עם הודעה על תקלה ובקשה להפעיל restart במחשב (החברה דיווחה שמשתמשי MAC ו לינוקס לא נפגעו).

התקלה גרמה לשיבושים בדרגות שונות של חומרה בסקטורים שונים ברחבי העולם ובישראל, לרבות בנקים, בתי חולים, קופות חולים, חברות תעופה, גופים קמעונאים, ובעיות בקווי חירום.

מנכ"ל החברה פרסם הודעה כמה שעות לאחר האירוע בה הבהיר שלא מדובר באירוע ביטחוני או במתקפת סייבר, הסביר כי הבעיה זוהתה, בודדה, החברה שיחררה תיקון והלקוחות הופנו לפורטל התמיכה של החברה.

גם מערך הסייבר הלאומי עדכן שלא מדובר במתקפת סייבר. על פי הודעת מערך הסייבר "בשעות אלו תקלה טכנית עולמית משפיעה על מערכות טכנולוגיות רבות ברחבי העולם, כמו גם בישראל. חברת הטכנולוגיה CrowdStrike הוציאה הבוקר התרעה טכנית בנוגע לבעיה משמעותית המשפיעה על מערכות Windows ברחבי העולם".



סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

על פי הדיווחים נראה שמקור התקלה בעדכון תוכנה תקול ששחררה החברה ללקוחותיה אשר הותקן באופן אוטומטי אצל הלקוחות, שרבים מהם דיווחו על בעיה.

עד כה לא ברור האם התיקון אכן פותר את הבעיה, האם מתאים לכל הלקוחות, האם נדרשת התקנה ידנית בתחנות הקצה ומהן השלכות התקלה והתיקון.

הטיפול באירוע רחוק מלהסתיים, היקף הנזקים אינו ברור, ואנו מניחים שיתוחקר ותופקנה מסקנות לרבות ביחס להתנהלות החברה ואחריותה המשפטית.

האירוע מחדד לדעתנו את הצורך בניהול סיכונים במערך טכנולוגית המידע - IT של ארגונים, בראש ובראשונה כתובנה עסקית הכרחית וכן כדרישה רגולטורית שבצידה אחריות של נושאי משרה (והכל בהתאם לדינים החלים על ארגונים בתחומים שונים). מובהר כי ביחס לגופים שהמחוקק זיהה שלגביהם ישנו סיכון גבוה, קיימות הוראות ייעודיות.

ארגונים נסמכים יותר ויותר על פלטפורמות דיגיטליות במהלך העסקים הרגיל שלהם. זהו תהליך בלתי נמנע שלו יתרונות עסקיים רבים אך בצידו אחריות לניהול הסיכון.

התקלה של חברת CrowdStrike מדגימה את הצורך במדיניות הוליסטית של הארגון בהגנה על נכסי המידע שלו והמשך ניהול תיקין של עסקיו הן בעבודה מקומית (on Prem), הן בשימוש בפלטפורמות ענניות (ענן ציבורי ופרטי), והן בעבודה היברידית. כל ארגון, בהתחשב בסיכונים שניצבים בפניו וברגולציה שחלה עליו, נדרש לגבש:

- תוכנית המשכיות עסקית (BCP) שמתאימה לא רק לאירועים ביטחוניים, סייבר ומגפות (כפי שהדגימה הקורונה), אלא גם לתקלות טכניות אשר מאפשרות לארגון להתאושש במהרה מכל אירוע כזה, וכוללת בין היתר: זיהוי גורמי סיכון, גיבוש אסטרטגיית מניעה והתאוששות מכשל (DR), חלוקת אחריות ותפקידים בארגון (לרבות צוות ייעודי לניהול המשבר), תוך מתן הנחיות ברורות בהתאם לתרחישי סיכון שונים, הטמעת התוכנית בארגון, תרגול וניטור.
- מערך הסכמים עם ספקי מוצרים ושירותים שכולל התייחסויות מתאימות בין היתר לאחריות הספקים וחלוקת האחריות ביניהם, עמידה בסטנדרטים בינלאומיים (כגון ISO 27001), רמת שירות נדרשת (SLA) לרבות זמינות המערכת (כולל מערכות ענן), וזמני טיפול בתקלות (התייחסות לסוגי תקלות, מעקפים workarounds), קביעת מדדים (KPIs), סעדים לארגון במקרה שהספק לא מספק מענה מתאים, שליטה בעיתוי ואופן ביצוע עדכונים ושדרוגים (מרחוק/on prem/בסביבת



סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

באר שבע
גב ים, רחוב האנגריה 77
ט. 03-6071450
פ. 08-6155780

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

ססט), בדיקות והבטחת איכות, גיבויים, זמינות צוות ייעודי מתאים של הספק למתן שירות וניהול אירועי משבר, אבטחת מידע ופרטיות, בקרות ופיקוח של הארגון.

- מדיניות ונהלי עבודה בקשר עם מערכות מידע מול גורמים פנימיים בארגון ומול גורמים חיצוניים לקוחות וספקים (בהיבטים טכניים ולוגיסטיים והיבטים משפטיים).

נשמח לסייע בגיבוש מדיניות כאמור והתאמת מדיניות קיימת לרגולציה במציאות המשתנה.



עו"ד אלון טבק אבירם, שותף
ראש מחלקת הייטק, טכנולוגיה
והון סיכון (משותף)
alont@agmon-law.co.il



עו"ד אסנת סרוסי פירסטטר, שותפה
ראש מחלקת הייטק, טכנולוגיה
והון סיכון (משותפת)
osnat@agmon-law.co.il



סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948