Read IT Now
מתפרסם מאז שנת 1999

הוגשה תביעה ע"י חברה ישראלית שנפגעה מדרישת כופרה [Ransomware]

02.02.2020 15:36

קטגוריות: אבטחת מידע/סייבר משפט

לבית-המשפט המחוזי בתל אביב הוגשה לפני מספר ימים תביעה מטעם חברה אשר נפגעה בדרישת כופרה [Ransomware].

בכתב התביעה, שהוגש בידי עורכי הדין דורון אפיק ויאיר אלוני [אפיק ושות', עורכי דין], נאמר בין היתר כי התובעת עוסקת בפיתוח פלטפורמות דיגיטליות. "**חלק מהותי ביותר מעסקי התובעת מבוסס על מערכות המחשוב שלה ועל יציבותן והגנתן מפני פגיעה חיצונית וכל השבתת מערכת משמעה נזקים מיידיים בסכומי עתק**".

ביולי 2016 נחתם הסכם בין התובעת לבין החברה הנתבעת "אשר על פי מצגיה עוסקת במתן שירותי אחסון וניהול שרתים. ההסכם היה למתן שירותי IT, שירותי אינטרנט וטלפונים וכן שירותים נוספים".

"במהלך ינואר, 2017, עם גידול בהיקפי הפיתוח ומעבר לפיתוח עצמאי, החלה החברה לבחון התקשרות עם ספק חיצוני אשר יספק פתרון כולל ורציני, המתאים להיקף הפעילות, בכל הנוגע לשירותי אירוח, אחסון דאטה ושירותי אבטחת מידע של כלל תוצרי הפיתוח והקניין הרוחני של החברה ובכלל זה, של מאגר המידע של החברה (הכולל מידע מסחרי בעל ערך רב כגון: פרטי לקוחות, פרטי עסקאות, היסטוריית התקשרויות וכו'). בתוך כך, פנתה החברה לקבלת הצעות מספקים מתאימים".

במהלך בדיקה זו מנכ"ל הנתבעת פנה אל מנכ"ל התובעת, ביניהם יש היכרות מוקדמת, "ופתח במסע שכנועים כדי להביא לכך שהתובעת תעבוד עם הנתבעת תוך שהוצגו בפני התובעת מצגים רבים אודות איכות השירות הניתן על ידי הנתבעת ובכלל זה, מתן פתרון כולל תחת קורת גג אחת (One stop shop)".

מנכ"ל החברה הנתבעת "הבהיר והדגיש (ועל בסיס מצגים אלה גם הסכימה התובעת לשכור שירותי הנתבעת) כי הנתבעת 'מעסיקה מומחים היכולים לספק את כל פתרונות התקשורת והמחשוב האפשריים' וכן כי על מנת לאפשר 'שרידות ונייידות גבוהה' קיימת פריסה בחמש חוות שרתים בישראל. הוא הוסיף ואמר כי הנתבעת מספקת לארגונים אסטרטגיים שירותי קישוריות אינטרנט "שרידה ומאובטחת".

לדברי כתב התביעה, "ביום 17.10.2019 בשעה 09:00 גילו מספר עובדות של החברה לראשונה שהן לא מצליחות לתפעל את מערכות ניהול המידע של התובעת. בד בבד, ולאחר בדיקת מתכנת של החברה, מתברר כי אין הגישה לשרתי החברה".

"בשעה 09:30 התקשר המנהל הטכנולוגי של התובעת למספר נייד שנתנה הנתבעת (מספר שהוביל ישירות לקבלן המשנה). שם נמסר לו כי הייתה פריצת אבטחת במהלך הלילה וכי הנושא בטיפול תוך שהוא מתחייב לעדכן את החברה בהמשך".

לאור בהילות העניין, ובשל השבתה מוחלטת של העבודה, בשעה 10:15 התקשר המנהל הטכנולוגי של התובעת שוב כדי להתעדכן ולקבל מידע באשר למהות התקלה החמורה. בשיחה זו נמסר על ידי קבלן המשנה של הנתבעת כי מדובר באירוע כופר (מתקפת סייבר בו מוצפנים הקבצים כאשר שחרורם מותנה בתשלום כופר לגורמים עלומים, תוך איום שאם לא יעשה כן כל הקבצים יושמדו)".

"עת התבררה חומרת המצב וכי אין המדובר ב'תקלה' טכנית שגרתית אלא אירוע אבטחה חמור במיוחד, פנתה החברה מיידית לקבלת סיוע מ- BugSec, חברה המומחית להגנה מפני מתקפות סייבר. עוד באותו בוקר התקיימה שיחת ועידה משותפת בהשתתפות אנשי אבטחת המידע של BugSec [...] בשיחה זו נדרש קבלן המשנה של הנתבעת להעביר את השרת, במצבו הפיזי כמות שהוא, AS IS, לידי BugSec לצורך ביצוע חקירה פורנזית מקיפה".

"כמו כן, במהלך השיחה ובעקבות ניסיונות בירור מצד BugSec התברר כי אירוע הפריצה נעשה ברמת 'הקלאסטר' (כך שלא היה ברור אם כלל השרתים המצויים תחת אותו נתיב רשת נדבקו במתקפת הכופר או מדובר בהדבקה נקודתית של השרת החי של החברה בלבד). לאור זאת, על מנת להקטין נזקים ולאפשר חזרה לשגרת עבודה מהירה ככל הניתן, נתבקש קבלן המשנה לחדש את העבודה באמצעות שרתי השכפול (הרפליקציה) שנועדו לשמש כגיבוי במצבים כגון אלה".

"[...] לתדהמת החברה התברר כי השרת הוירטואלי אף הוא נפגע באירוע האבטחה במקביל לפגיעה השרת הפיזי, כל זאת בניגוד גמור להתחייבות מפורשות של הנתבעת ובניגוד לכל סטנדרט אבטחה סביר ומקובל, לפיו נהוג לאחסן את השרתים בחוות נפרדות

כדי למנוע אובדן מוחלט של מידע [...] משנודע כי אין גיבוי, לא היה מנוס אלא לחדש את הפעילות באמצעות שרת נקי וללא דאטה ובכך להקטין במעט את הנזק שנגרם".

"[...] התובעת הייתה בקשר בכל אותה העת מול הנתבעים כאשר שוב ושוב הוצג בפניה מצג כי הנושא ייפתר בכל רגע. יודגש, עיכוב זה הביא בין היתר לכך כי התובעת נאלצה לבטל את האירועים של אותו יום (ולבסוף גם את אירועי היום שלמחרת), לפצות ולזכות את כלל לקוחותיה בגין האירועים שבוטלו, והכל לצד אי היכולת לעבוד באופן סדיר ולקחת הזמנות חדשות. מעבר לנזק הכספי, מדובר בנזק מוניטין אדיר לתובעת – נזק שיכול היה להימנע בקלות אילו הנתבעת הייתה מודיעה לתובעת מייד עם קרות האירוע ומטפלת באירוע באופן מיידי".

לאחר סוף השבוע ובצאת החג, ועם חזרה לעבודה, ולאחר ש"התובעת הבהירה באופן חד משמעי שהיא דורשת שהשרת יועבר אליה במצבו כפי שהוא" כדי לבצע בדיקה פורנזית, התברר בהמשך התהליך כי "השרתים עובדים על גבי השרת הפיזי הישן, לאחר שזה פורמט, וזאת בניגוד גמור לדרישות והנחיות התובעת וללא ידיעתה. פירמוט השרת לא רק מונע הצלת החומר שעליו והקטנת הנזק, אלא גורם נזק ראייתי כבד לתובעת באשר הנתבעת וקבלן המשנה השמידו במכוון (ותוך הפרת דרישה מפורשת של התובעת לקבל את השרת) את כל הראיות".

"מעבר לעובדה כי מדובר בהפרת התחייבות חוזית, מדובר בהפרת אמון חמורה כאשר המשמעות המעשית היא כי התובעת אינה יכולה כעת לבצע חקירה פורנזית בשרת החי כדי להבין את הסיבות שהובילו להדבקת השרת החי בוירוס הכופר ובכך נגרם לה נזק ראייתי חמור".

"עצם התפשטות הוירוס לכל קלאסטר השרתים, מעלה חשד גבוה לכשל אבטחת מידע חמור, הואיל והתפשטות הוירוס אפשרית מבחינה טכנית רק אם בהתקיימות קשר בין השרתים החיים השונים או ככל שבשרת החי של התובעת הוחזקו גיבויים של צדדים שלישיים, בניגוד גמור לנוהלי אבטחת המידע והתחייבויות החוזיות, אך כעת עם פירמוט השרת החי נמנעה מהתובעת הזכות לביצוע חקירה פורנזית אשר בוודאי הייתה שופכת אור על נסיבות האירועים".

"הואיל ושרתי הגיבוי (השכפול והגיבוי היומי) עדיין נותרו מוצפנים, אספה התובעת שרתים אלו על מנת לבצע חקירה פורנזית, זאת, בד בבד לביצוע חקירת האירוע מצד קבלן המשנה של הנתבעת, כאשר סוכם כי לאחר שיתקבלו המסקנות תיערך ישיבה משותפת לצורך שיתוף במסקנות הבירור".

"עם זאת, מזה מספר חודשים מנסה התובעת לקבל תשובות ומענה מקצועי באשר לתוצאות החקירה והבירור שנעשה על ידי הקבלן המשנה, אך למרבה הצער זכתה התובעת לשיתוף פעולה מינימלי כאשר דו"ח החקירה לא הועבר לעיניה וזאת עד למועד זה".

לדברי כתב הטענות, "המדובר באירוע אבטחה חמור בו לכאורה 3 מעגלי עבודה ושרידות נפרצו (שרת חי, שרת שכפול ושרת גיבוי יומי) כאשר כל שרת היה אמור להיות חיבור לרשת חיצונית נפרדת עם גישה פרטית לאינטרנט עם מערך אבטחה משלו, כך שברור כי אילולי קיומו של מחדל אבטחה חמור מצד הנתבעת כלל לא היה נגרם הנזק לחברה. עצם גרם הנזק הראייתי מעלה חשד כבד כי כלל לא נפרצו שלושה מעגלי אבטחה אלא שאלה לא היו קיימים כלל!".

התובעת אומרת עוד כי "למען השלמת התמונה, יצוין כי בחודש ינואר נעשה ניסיון כן לפתור את סכסוך מחוץ לכותלי בית המשפט אך ניסיון זה לא צלח".

"מאגר המידע של התובעת שוחזר באופן חלקי בלבד (בינתיים רק לחלק מהשנים 2018-2019) וכך אבד מידע אדיר שנצבר במשך כ- 6 שנות פעילות – כ- 80% מתקופת הפעילות של התובעת. בתובעת הושקעו עד היום מיליונים רבים של שקלים, לרבות ביצירת מאגר מידע זה והתובעת מעריכה את שוויו בסכום המוערך על הצד הנמוך בסך של 2,500,000 ש"ח."

הערה: ההדגשות מופיעות במקור.