הערכות התעשייה לתקיפות סייבר – תובנות מתקיפות סייבר משמעותיות על מספר חברות בתחום הכימיקלים והאלומיניום בעולם במהלך מרץ 2019

בשבוע של ה 20 למרץ 2019, התרחשו מספר התקפות סייבר מתוזמנות ומתוכננות מול מספר חברות בינלאומיות בתעשייה, ההתקפה המסוקרת ביותר הייתה מול חברת ייצור האלומיניום Norsk Hydro, החברה עדיין מתאוששת מההתקפה ולא חזרה לפעילות מלאה

להלן מתוך הסקירה של חברת אבטחת מידע וסייבר הישראלית Clear-Sky בניהולו של בועז דולב:

אודות התקיפה

לנוזקה אין מנגנון הפצה. הנוזקה הופצה ככל הנראה לאחר שהתוקפים הצליחו להשיג אחיזה ב- Active Directory של התאגיד. בתאריך ה 19.3 ככל הנראה מספר דקות לאחר השעה 12 בלילה, החל תהליך ההצפנה במספר רב של מחשבים ושרתים. בעקבות כך, מחשבים ושרתים רבים (לא ברור המספר) פסקו לתפקד. חלק מתהליך התקיפה היה ביצוע של Logout לעובדים ונעילה של חשבונותיהם. כך נמנעה היכולת מאנשי המחשוב לטפל באירוע וככל הנראה החברה ביצעה ניתוקים פיזיים של רשת התקשורת על מנת לנסות ולעצור את פעילות התקיפה. לפי ה-Cert הנורבגי " NorCert" נעשה שימוש בתקיפה בכופרה לא ידועה מסוג LockerGoga.

להבנתי זו הייתה תקיפה מתוכננת ומשולבת במספר חברות מתוך אינטרס לגרום לנזק תפקודי וכלכלי עם מסר לעולם המערבי ולא תקיפה מקרית של ארגון פשע כזה או אחר, חברות בתעשייה שלנו יכולות ועלולות להיות יעד לתקיפות דומות בעתיד

המשמעות לתעשייה שלנו: צורך בנקיטת מספר מהלכים

בטווח המיידי:

לעקוב אחר ההתראות והפרסומים של ה CERT הלאומי במערך הסייבר הלאומי וליישם את ההמלצות הניתנות, ככל שרלוונטיות לכל ארגון

הפרדה רשתית - הקפדה על הפרדה לוגית או פיזית בין רשתות הייצור לרשת העסקית וקישורים מאובטחים בין הרשתות

להקפיד להוריד ולהתקין עדכוני אבטחה בהתאם להמלצות יצרן בשרתים ותחנות קצה בדגש על הרשת העסקית

הרשאות יתר - צמצום מספר בעלי הרשאות יתר ושמירה על רמת אבטחה גבוהה למשתמשים בעלי הרשאות אלה

הערכות להתמודדות עם אירוע סייבר והתאוששות – ליצר תכנית פעולה והערכות למקרה סייבר מהותי עם מעורבות פעילה של ההנהלה הבכירה, כולל תרגול עלייה מגיבויים ומה עושים ללא מערך מחשוב לזמן מוגבל

מערך אבטחה טכנולוגי – לוודא שימוש יעיל ומלא ביכולות של פתרונות וציוד שכבר נרכש

בטווח הבינוני:

להטמיע ולפעול בהתאם למתודולוגיה (תורת ההגנה בסייבר לארגונים) של מערך הסייבר הלאומי

ברשת העסקית – העברת חלק מהפעילויות לשירותי ענן ברמת אבטחה גבוהה להעלאת השרידות

סיכוני סייבר – ניתוח הסיכונים הנובעים מאירועי סייבר לנכסי המידע של הארגון והכנסתם לתהליך בקרת ניהול סיכונים של החברה

אנו נשמח לדיאלוג ומענה לשאלות בתחום איומי הסייבר והמענה

אלברטו (דטו) חסון

deto@industry.org.il