הפתרון למתקפות הכופרה

במציאות בה אנו נמצאים, ברור כי שחזור מלא של הנתונים
הינו המפתח להתמודדות עם מתקפות סייבר

DELL CYBER RECOVERY

הגנה תשתיתית כנגד איומי סייבר.
פתרון יעיל ביותר, המנותק מכל מערכות הארגון.

גל מתקפות הסייבר ששוטף את העולם כבר לאורך תקופה, מוכיח עובדה מאוד פשוטה – קיים אתגר לחסום במאת האחוזים את יכולת הפריצה למערכות הארגון ולכן חייבים לחשוב על היום שאחרי ולדאוג למערכת שחזור נתונים שתהיה ה"מגן האחרון" ותאפשר לארגון לחזור במהירות המרבית לתפקוד מלא.

בשנת 2020 התרחשו כ- 304 מיליון אירועי כופרה (Ransomware) ברחבי העולם, כל 11 שניות ארגון נפרץ. **כ- 86% מכל מתקפות הכופרה נובעות ממניעים כלכליים - כך שאופי החברה לא רלוונטי כלל. אי אפשר להתעלם מהנתונים הללו. מנגנוני האבטחה הקיימים דומים לסכר ענק הנמצא כל העת תחת מתקפה.** 'האקרים' מבצעים נסיונות פריצה כל העת, וחברות האבטחה מייצרות עדכוני תוכנה למניעת פריצה. יחד עם זאת, למרות כל המאמצים ועדכוני התוכנה, אנו עדים כל יום לחברות שהסכר שלהן נפרץ והמידע שלהן הוצפן. זו המציאות - לחברות קטנות וגדולות כאחד. **אז מה עושים לאחר שהסכר נפרץ וכל המידע הוצפן?**

בחברת Dell Technologies הבינו שהמפתח במניעת אסון עבור הארגון, במקרה של מתקפת סייבר, הוא ביכולת הטובה והמהירה ביותר שלו לשחזר את הדאטה שהוצפנה בתקיפה.

פתרון Dell Cyber Recovery מספק שכבת הגנה נוספת לתשתית הגיבוי ומייצר 'כספת' בלתי חדירה - Cyber Vault, סגורה ומסוגרת, השומרת על הגיבויים בסביבות הקריטיות ביותר של הארגון, מפני מתקפות סייבר. רק בעת הצורך ניתן לפתוח אותה ולהשתמש בנתונים השמורים להחזרת פעילות הארגון למסלולה.

דו"ח גרטנר ממליץ על היכולות הקיימות ב- Cyber Recovery כקו ההגנה העיקרי למתקפות כופרה. זאת ועוד, שתי ההמלצות הראשונות של מערך הסייבר הלאומי הן: "וודאו קיום יכולת גיבוי והתאוששות מהירה של הארגון, בדגש על עותק עצמאי שאינו מחובר לרשת הארגון ובצעו ניטור מוגבר, בדגש על אנומליות סייבר".

חררדו רודניק, ארכיטקט ראשי ומנהל מחלקת פריסייל באגף המכירות של מלם תים: *"כל חברה דואגת שיהיו לה עותקי גיבוי המיועדים לשחזור עתידי, אבל השאלה הגדולה היא, היכן מאחסנים את הגיבויים הללו. רוב החברות מאחסנות אותם בתוך הדאטה סנטר שלהן, כך שלמעשה, בזמן פריצה, גם הם חשופים, שכן, ברגע שהפורצים מקבלים גישה לדאטה של הארגון, הם יכולים להגיע בקלות גם לגיבויים. Dell Cyber Recovery, באמצעות Cyber Vault, מעניק שכבת הגנה נוספת, המהווה את ה"קיר" האחרון בין הפורצים לבין המידע".*

איך הפתרון עובד ומדוע הוא נחשב למהפכני?

"הרעיון מאוד פשוט". אומר **אבי שוורץ, Data Protection Account Executive בחברת Dell Technologies:** *"לנתק את ה'כספת' מכל קשר לעולם החיצון. הפתרון מבוסס על מערכת ה- Backup to Disk של Dell מסוג Data Domain המשווקת למעלה מעל 15 שנה ומחזיקה כיום כ- 50% מנתח השוק העולמי בתחום זה. ניצלנו את יתרונות המוצר וביצענו בו שינויים, שהופכים אותו לכספת, שהיא סביבה מוגנת, המופרדת לוגית מאתר הייצור באמצעות מנגנון Air Gap, המנתק*

דו"ח גרטנר ממליץ על היכולות הקיימות ב- CYBER RECOVERY כקו ההגנה העיקרי למתקפות כופרה. זאת ועוד, שתי ההמלצות הראשונות של מערך הסייבר הלאומי הן: "וודאו קיום יכולת גיבוי והתאוששות מהירה של הארגון, בדגש על עותק עצמאי שאינו מחובר לרשת הארגון ובצעו ניטור מוגבר, בדגש על אנומליות סייבר".

פיזית את הכספת מהרשת הארגונית ומאפשר תנועה חד-כיוונית מצד הכספת בלבד, בזמנים קבועים וקצרים. לאחר שעותקי הגיבוי עוברים מאתר הייצור לכספת, הם ננעלים ב- Retention Lock ומאפשרים לייצר immutable copies של המידע. הרפליקציה עצמה מתקיימת בין שתי מערכות Data Domain ולמערכות הארגוניות אין שום שקיפות למנגנון זה – לא לעצם קיומו ולא לתהליך השוטף. למעשה תוכנת הגיבוי כלל לא מודעת לנוכחותו של אתר הכספת. כמובן שהחסכון האדיר בנפחים של מערכת ה- Data Domain נשמר גם פה, דבר המאפשר פתיחת הרפליקציה לטווח זמן קצר במיוחד. לאחר שהמידע עבר מאתר הייצור לכספת, מיושם ה- Air Gap אשר מונע את הקשר בין הכספת לעולם החיצון כאשר כל האורקסטרציה מתבצעת מצד הכספת".

למי מתאים הפתרון?

"בשנה האחרונה ביצעה מלם תים מספר פרויקטים מורכבים, בעיקר בקרב לקוחות בינוניים וגדולים, בעלי מידע רגיש וקניין רוחני, אשר מבחינתם איבוד הנתונים הוא קריטי!" אומר חררדו רודניק ממלם תים. "אנחנו חווים צורך גדול מאוד מהשטח, מאחר וכולם כבר מבינים שזו לא שאלה של 'האם', אלא 'מתי' תקרה הפריצה, כך שחייבים לבצע מהלך של התגוננות אקטיבית. המצב האוטופי הוא להצליח לקבל התרעה ולעצור את המתקפה לפני שהיא קורית, אבל אין להסתפק בכך, על מנת להבטיח שבכל מקרה, הידע שנצבר בחברה, אשר לא יסולא מפז, לא יאבד לנצח. אנחנו בהחלט יכולים להגיד, שבאמצעות Dell Cyber Recovery, הצלנו את החברות, אשר היו אף עלולות להימחק כליל, ללא שחזור המידע".

מדוע גיבוי פיזי לא יכול לשמש כפתרון להגנה כנגד איומי סייבר?

"קלטת המופרדת פיזית אינה פתרון להגנת סייבר, מאחר ולא ניתן להריץ אנליזות על המידע הנמצא בקלטת ללא שחזור כל המידע ולכל פעולה שכזו יידרשו זמן רב והשקעה רבה בתשתיות. בנוסף, אנו יודעים כיום כי ישנם וקטורי תקיפה מסויימים הנמצאים ב'מצב שינה' ומתפרצים רק במועד עתידי. ללא מערכת פרו-אקטיבית המנתחת את המידע ויודעת לשחזרו באזור נקי, הסיכון בשחזור נוזקת הצפנה גבוה מאוד".

מסכם חררדו: *"לא מספיק רק לשמור ולנטר את המידע הנכנס לארגון, אלא יש לבצע גם שמירת עותקי גיבוי למידע הקריטי ביותר באופן מוגן מפני מתקפת סייבר, למקרה של כשל מלא.* ***אנו במלם תים מציעים ללקוחותינו, באמצעות יישום של מערכות Data Domain, יחד עם יכולת Cyber Recovery של Dell, פתרון מלא, אוטומטי ובאינטגרציה מלאה לתשתית הקיימת, הכוללת מספר רב של כלים לגיבוי ושחזור יעילים, מהירים ובטוחים.*** *יישום הפתרון מספק הגנה תשתיתית כנגד מתקפות סייבר, באופן קל ליישום, תוך שמירה על המידע הקריטי ביותר של הארגון".*

בשנת 2020 התרחשו כ- 304 מיליון אירועי כופרה (Ransomware) ברחבי העולם. כל 11 שניות ארגון נפרץ, ו-86% מכל מתקפות הכופרה נובעות ממניעים כלכליים - כך שאופי החברה לא רלוונטי כלל.