שחזור מידע - טכנולוגיה כנגד כל הסיכויים

מאת: יואב זילברשטיין

להכנס לאווירה

כדי להכנס לעולם שחזור המידע אשתף אותכם בחוויה שעברתי לפני שבועיים: אל מעבדתנו הגיע לקוח עם שרת הכולל RAID (מערך דיסקים פשוטים בעברית) - 4 דיסקים קשיחים. הלקוח הינו בעלים של חברה גדולה העוסקת בשווק סחורה חקלאית לכל העולם. 2000 דונם גידולים חקלאים שזה עתה נקטפו, בשיא העונה, ומחכים למשלוח ללקוחות שונים מעבר לים. "I'm Broken" אומר הלקוח, כל ההזמנות שלנו - נמצאות בתוך השרת, אין לי מושג איזה פלפל לשלוח לאיזה לקוח. סחורה במיליונים עומדת להזרק לפח. כאוס מוחלט.

בדיקה של כמה שעות מגלה שיבוש כבד במערך ה-RAID. אין קבצים, אין נתונים ואין סחורה למכור. השרת מגיעה אלינו לאחר ניסיונות שחזור של מספר גורמים, בהם אנשי ה-IT של החברה, גורמים פנימיים וחיצוניים. בתהליך נעשו הרבה מאוד שגיאות, דריסה של חומר, איפוס ובנייה מחדש של מערך ה- RAID, בקיצור בשפה שלנו "Total loss".

אחרי יומיים זה נראה די אבוד. הלקוח מרגיש שעולמו חרב. אנו מנסים שיטות שונות לשחזור מערך הנתונים שאבד. בשעת לילה מאוחרת מגיע רגע הבינגו. יש מידע, והמידע ניתן לשחזור. הלקוח מעודכן. קשה לתאר את עוצמת השמחה של הלקוח. מהצד שלנו אף פעם לא ניתן להתרגל לתחושת הסיפוק, התחושה הזו תמיד נותנת אנרגיה למקרה הבא.

במקרה זה הצלנו הרבה מאוד חקלאים שהופכים פלפלים צהובים למזומנים, עבודה לא פחות מסובכת מלשחזר מידע.

אז מה זה שחזור מידע?

שחזור מידע היא נישה בעולם ה-IT, שמטרתה לשחזר מידע שאבד. הלקוחות הם החל מחברה מסחרית שאיבדה נתונים פיננסים או מצגות חשובות, דרך בתי חולים שאיבדו נתונים רפואיים, אוניברסיטות שאיבדו מחקרים ועד לקוחות פרטיים שאיבדו תמונות דיגיטליות מהטיול האחרון לסין.

המדיה הדיגיטלית בה מאוחסנת 99% מכמות המידע בעולם, היא דיסק קשיח, פחות או יותר אותה טכנולוגיה כבר 30 שנה, עם המצאות חדשות שבאות מידי פעם. ראש קריאה / כתיבה שטס מעל פלטה במהירות עצומה. אבל הדיסקים הקשיחים לא לבד, גם מדיות נוספות שייכות לעולם האחסון, כונני SSD למשל אשר נמכרים יותר ויותר בשנים האחרונות, DISK ON KEY לסוגיו השונים, כרטיסי זכרון, דיסקטים, וגם קלטות גיבוי אשר עדיין בשימוש רחב בארגונים. גם טלפונים סלולריים הופכים בשנים האחרונות לדומיננטיים. הטלפון הופך להיות המחשב הבא. יותר ויותר מידע עובר היום לטלפון הסלולרי - תמונות, סרטים ועוד.

מטרת השחזור היא להביא כמה שיותר מהר להמשכיות שימוש של הלקוח. לנושא זה משמעות כספית רבה. הנזק הנגרם לארגונים בעולם כתוצאה מאובדן מידע הוא אדיר, ומוערך במיליארדים רבים בכל שנה.

שחזור פיזי מול שחזור לוגי

עולם שחזור המידע מורכב משני נושאים עיקריים: **שחזור פיזי** ו**שחזור לוגי**.
שחזור פיזי הוא תהליך שחזור של מדיה אשר נפגעה, בעיקר מתקלות שונות כגון פגיעה בפלטות הנתונים, תקלה בראשי קריאה / כתיבה או אלקרוניקה. קיימים גם ארועים חריגים של פגיעות כתוצאה משריפות, הצפות, התרסקויות של כלי טיס הכוללים בתוכם גם מדיות שונות, ארועי לחימה שונים או ארועי טרור.

וקצת להווי המקצוע - כמעט כל חודש מקבלים סיטואציה מוזרה לשחזור: למשל דיסק שנזרק במריבה בין בני זוג לתוך נחל הירקון, כלב שלעס את כרטיס הזכרון, ילד ששיחק עם מגנט חזק ופגע במחשב העבודה של אביו ועוד מקרים מוזרים אחרים.

תהליך השחזור הפיזי כולל שימוש בטכנולוגיות מגוונות - החל ממכונות מיוחדות המאפשרות קריאה של פלטה פגועה, עבודה אלקטרונית נרחבת, וכן ביצוע בנייה מחדש של אזור היצרן (Service area). כמו כן,

נעשה שימוש במאגר אדיר של חלקי דיסקים (בעולם קיימים מעל 80,000 סוגים שונים של דיסקים קשיחים, נכון לשנת 2011) לצורך החלפה של חלקים שונים שניזוקים בתוך מכלולי הדיסק.

שחזור לוגי הוא תהליך של שחזור מתוך מדיה תקינה, שבה אגור מידע אשר שובש או נמחק. מסד נתונים פיננסים משובש של חברה, או ארוע שבו נמחקו בשוגג מסמכים חשובים. תהליך השחזור הלוגי כולל שחזור קבצים, ע"י שימוש בכלי תוכנה מתקדמים. מעבדה מקצועית לשחזור מידע אוגרת בתוכה מעל 1000 כלי תוכנה יחודיים המסוגלים לטפל בסיטואציות שחזור מידע שונות. קיימים כלים מסחריים שונים המאפשרים שחזור לוגי, אולם מעבדות מקצועיות ישקיעו במו"פ של כלי תוכנה מיוחדים אשר מאפשרים שחזור גם כאשר הכלים "הרגילים" לא עובדים.

איך משחזרים קובץ שנמחק?

כאשר קובץ נמחק (למשל מחיקה מתוך סל המחזור או כתוצאה מביצוע FORMAT לדיסק), הוא עדיין נשאר לרוב אגור בתוך הדיסק. למעשה, בשעת המחיקה, רק הגדרות שונות של הקובץ משתנות, ומערכת הקבצים מפנה ברשומות שלה את האזור בו אגור הקובץ. באמצעות כלי תוכנה מתאימים, ניתן לאתר את שרידי רשומות הקבצים, ולהגיע לרוב לקובץ המחוק ולאתרו בצורה שלמה.

שחזור חקירתי

לשחזור מידע יש גם אספקטים נוספים - שחזור על רקע חקירתי או משפטי. בשפה המקצועית זה מכונה Computer Forensics. הצרכנים של שרות כזה הם לקוחות ממשלתיים, בתי המשפט, חברות מסחריות או לקוחות פרטיים. השחזור החקירתי שונה מהשחזור הרגיל - כבר לא מספיק לשחזר את המידע שהיה גלוי בדיסק. יש צורך לשחזר מידע מחוק, לתאר מתי הארועים התרחשו, מי עשה אותם, ובשורה התחתונה לספק את סיפור המעשה וזאת לצורך הבאת ראיות לתהליך משפטי.

השחזור החקירתי בנוי משני חלקים - איסוף ומחקר. איסוף הינו ביצוע העתקים משפטיים באמצעות כלי תוכנה וחומרה מתאימים, המתעדים נאמנה את תוכן המדיות הנדרשות. השלב השני הוא המחקר - ניתוח הראיות, שחזור הקבצים הגלויים והמחוקים, חיפוש אחר מילות מפתח יחודיות הקשורות למקרה, ביצוע שאילתות מורכבות לצרכים המשפטיים ועוד.

השמדת מידע

השחזור החקירתי דורש לעיתים ביצוע השמדת מידע, למשל אם נמצאו ראיות בתוך דיסק קשיח של צד בסכסוך משפטי, יחד עם מידע לגיטימי שלו. לעיתים יש לבצע מטעם ביהמ"ש מחיקה בלתי הפיכה קבצים שנמצאו, כדי שניתן יהיה להשתמש עם קבצים לגיטימיים אחרים שנמצאים בדיסק. פעולות השמדת המידע נעשות באמצעות כלי תוכנה יחודיים ולעיתים גם ע"י חומרה יחודית המאפשר פגיעה בלתי הפיכה במידע.

פני העתיד

עולם האחסון עובר היום בהדרגה למדיות של זכרון בלתי נדיף - SSD. שחזור כונני SSD יהיה נפוץ יותר ויותר בעולמינו, אם כי יקח עוד מספר לא קטן של שנים בו עדיין הדיסק הקשיח ינצח, בעיקר בגלל יחס יחידת האחסון למחיר. עולם השחזור מתמודד גם עם נושא צפיפות פלטת הנתונים - כיום הנפחים של הדיסקים מגיעים עד 3TB לדיסק קשיח אחד. ההפרדה בין הסקטורים הופכת להיות קשה יותר, ונדרשות טכנולוגיות יחודיות לצורך ביצוע פעולות שחזור מורכבות בתוך הדיסקים הקשיחים.

הרגל צריכה נוסף שישתנה הוא ביטוח שחזור מידע. היום המודל העסקי הנפוץ הוא טיפול בלקוח במקרה חרום, ועלות שחזור שיכולה להיות יקרה. כיום קיים פתרון המאפשר ללקוח לרכוש Online ביטוח לשחזור מידע, במחיר זול מאוד (עשרות שקלים לשנה לכל דיסק קשיח). הרעיון שעומד מאחורי זה היא מערכת יחודית שפותחה, מבוססת פטנט עולמי ברישום, המאפשרת לזהות ולבדוק Online דיסקים לצורך הכנסתם לתוכנית ביטוח. מגמה זו תוביל תוך מספר שנים את יצרני הדיסקים ויצרני המחשבים להציע שרות משלים לביטוח שחזור מידע, בדומה לאחריות חומרה הניתנת היום בצורה רגילה לשנה עד 5 שנים. פרטים על התוכנית באתר www.safetter.co.il .

שיטת שחזור חדשה נוספת אשר תהיה נפוצה היא "שחזור מידע מרחוק". הטכנולוגיה כיום מאפשרת ביצוע שחזור מידע בחלק מהמקרים, ללא משלוח של הדיסקים למעבדה. שחזור שרת הכולל בתוכו מערך RAID מתבצע כיום באמצעות אתר Online Raid Recovery או באמצעות חברת Ontrack .

אודות המחבר

יואב זילברשטיין, מנכ"ל ובעלים של חברת טיק טק טכנולוגיות, חברה שנוסדה בשנת 1995 ומובילה את תחום שחזור המידע בישראל. פרטים אודות החברה באתר http://www.tictac.co.il