מסנכרנים את הזמן, מנטרלים את איומי סייבר

חור אבטחה ענק פעור בליבן הפועם של רוב רשתות המחשבים בישראל - הזמן. בין אם כתוצאה מחוסר הרגולציה או פשוט כתוצאה מסינדרום ה"ניתן לקבל את זה חינם מהאינטרנט, אז למה לשלם?", חברות וארגונים מסתכנים בסנכרון ממקורות לא מאובטחים, שעשויים לגרום לנזק בל ישוער | **עומר שרר, מנהל תחום סנכרון, פוקוס טלקום**

רוב רשתות המחשבים בחברות המובילות במשק הישראלי צורכות את הזמן שלהן מהאינטרנט ובכך מסכנות את הרשת שלהן למתקפת סייבר, את אמינות המידע שלהן ואולי גרוע בהרבה מכך - את המידע הרגיש ביותר של לקוחותיהם.

נתחיל במה שכבר כולם יודעים - אנחנו חייבים זמן מדויק בארגון. אם זה עבור אחסון נכון וסידור של כמויות המידע העצומות אשר זמין לנו היום (עידן ה"ביג דאטה" הבא עלינו לטובה), ואם זה עבור חתימות זמן מדויקות לטרנסאקציה פיננסית (התקינה העולמית מתייחסת לדרישת חותמת זמן מאובטח בכל העברה כספית בבנקים ובמסחר בורסאי). כך גם עם כל חתימה דיגיטלית, או תיעוד נכון של גישה לפרטי לקוח רגישים (מידע רפואי, פרטי כרטיס אשראי וכיוצ"ב), וכך גם עבור יישומי הצפנה ואבטחה הדורשים זמן. ולבסוף, ולא פחות חשוב, עבור תיעוד וניתוח אירועי התקפות סייבר. כמה מדויק? זו כבר שאלה יותר מעניינת. בעולם יש מספר תקנים רלוונטיים לנושא.

נתחיל מהתקנים "הקלים":

- **DFARS** - על כל ארגון אשר נותן שירותים לממשלה האמריקאית לתעד כל "תקרית סייבר" שהתרחשה עם חתימת זמן ממקור מאובטח.
- **SOX** - כל החברות הציבוריות בארה"ב חייבות בחותמת זמן על כל אירוע כספי (כגון הענקת מניות) למניעת backdating וכדומה.
- **GLBA** - כל הבנקים, חברות הביטוח, חברות אבטחה, וכל מוסד אחר המספק שירותים פיננסיים, חייבים בחתימת זמן מדויקת ממקור מהימן וביכולת לספק "שובל מעקב" (audit trail) המספק היסטוריה של הזמן המדויק של כל גישה לנתונים הרגישים של הלקוחות.
- **PCI-DSS** - כל עסק המאחסן נתונים ומספק שירותי סליקת כרטיסי אשראי חייב ביישום חתימות זמן ושובל מעקב אוטומטי על כל גישה לפרטיו של הלקוח.

התקנים המקשים יותר, אשר יכנסו לתוקף בשנה הקרובה, מגיעים מהעולם הפיננסי. רשות ניירות הערך האמריקאית (SEC rule 613) דורשת סנכרון של כל המחשבים בארגון סוחר ברמה של מילי שניה בודדת לזמן העולמי. רשות ניירות הערך האירופאית (ESMA MiFiD II) דורשת מכל ארגון הסוחר בני"ע סנכרון המחשבים ברמה של עד 100 מיקרו-שניות (!) לזמן העולמי. מלבד הגדרת הדרישות המאתגרות הללו, מוגדר גם שעל כל ארגון לעבור ביקורת תקופתית מהרשות לני"ע לוודא שאכן עומדת בדרישות.

ומה מוגדר בארצנו הקטנטונת? קיימת "המלצה" לחברות לאמץ תקנים מאירופה ומארה"ב (כמו PCI-DSS לאבטחת פרטי כרטיס אשראי) אך אין שום אכיפה על יישום התקן ובוודאי על נושא הזמן שהוא חלק אינטגרלי וחשוב מהתקן. אם יורשה לי לצטט את מנהל אבטחת המידע מאחד הבנקים המובילים בארץ: "אף אחד לא מכריח אותנו... לנו מספיק לדעת מתי נגמר היום כדי שנדע אם לבצע את הפקדת הצ'ק שלך היום או מחר".

חשיפה למתקפות

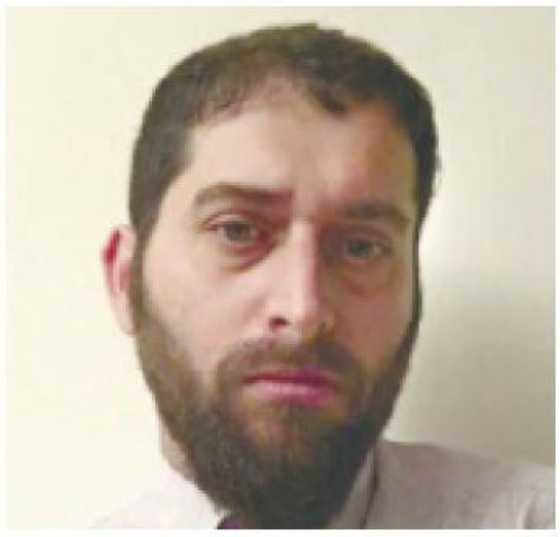
אז למה לא לסנכרן את הרשת שלנו מהאינטרנט? שאלה נהדרת. יש במדינת ישראל ובעולם כולו הרבה שרתי זמן (NTP servers) ציבוריים, אשר מטרתם היא לתת את הזמן המדויק לכל מי שמבקש. עם קצב הגלישה ההולך ועולה באופן קבוע ניתן אפילו לקבל את הזמן בדיוק יחסית טוב (מספר מילי-שניות בלבד מהזמן העולמי). נשמע טוב, אך יש לזה שלוש בעיות עיקריות:

- **חשיפה של הארגון למתקפת DDoS** - בעוד מחשב (או מספר מחשבים) בארגונינו מבקשים את הזמן מאחד השרתים הציבוריים, הם פותחים לרווחה את פורט 123 (הפורט בו אנו משתמשים לטובת הזמן - NTP). בשנת 2014 תועדה תקיפת ה-UDP amplification הגדולה עד כה: 4,529 שרתים תקפו מ- 1298 רשתות שונות מחשב של ספק שירותי תוכן באמצעות הפצצה שלו ביותר מ- 400 Gbps (400 ג'יגה ביט לשנייה).
- **זמינות מקור הזמן** - שרת ציבורי לא תמיד זמין והחיבור אליו לא תמיד זמין (לא סתם הוא חינם). אם הוא לא זמין לתקופה ממושכת, המחשבים ברשת שלנו "יסחפו" כאוות נפשם לפי השעון הזול מבוסס הבטרייה במחשב שלנו.
- **אמינות מקור הזמן** - זו אולי הבעיה הגרוע מכולן: כתובתם של השרתים הציבוריים ידועה לכולם וכל מי שמתאמץ קצת יכול לדעת בדיוק מאילו שרתי זמן ציבוריים הארגון שלנו מסונכרן. זה מאפשר להאקרים לבצע מתקפת Man in the middle קלאסית. כאן אפשר לנקוט בשתי גישות, האחת, ARP spoofing - ARP זה הפרוטוקול אשר מקשר בין הכתובת IP של מחשב לבין כתובתו הפיזית (MAC address). ניתן למעשה בשיטה זו להתחזות לכל מחשב ולענות במקומו על השאלה שלנו "מה שעה". שיטה נוספת היא DNS spoofing - אם שרת הכתובות הדינאמי, אשר אמור לנתב את בקשת הזמן שלנו לשרת זמן ציבורי, מנתב אותה לשרת מפוקפק, המחשב בארגוננו יקבל את הזמן מאותו שרת מפוקפק.

אז מה עושים? הפתרון הוא פשוט. להביא את מקור הזמן אל תוך הרשת שלנו. מעבר לנתוני מיקום מדויקים, מערך לווייני ה-GPS ומערכים מקבילים אליו (Glonass של הרוסים ו-Galileo של האיחוד האירופי) מסוגל להעביר לנו את הזמן בדיוק גבוה אלפי מונים מזה שניתן לקבל מהרשת. עם שרת זמן כדוגמת ה- Microsemi SyncServer S600 שיותקן ברשת שלנו, אנחנו יכולים להביא מקור זמן אל מאחורי ה- firewall המסונכרן ברמה של 15 ננו-שניות לזמן העולמי ובכך למנוע נזק עצום באלפי דולרים בודדים. עם פתרון משלים בצורת מערכת ניטור וניהול זמן של חברת פוקוס טלקום הישראלית, תוכלו גם לתכנן, לנטר ולנהל את הפצת הזמן בארגונכם עד רמת מחשב הקצה ולוודא שהמחשבים הקריטיים שלכם לא "מתבדרים" בזמן.

שירותי סנכרון ותזמון

קבוצת פוקוס טלקום הוקמה בשנת 1995 ע"י **אהוד שרר** במטרה לתת מענה לצרכים של חברת בזק בכל הקשור לסנכרון רשת התמסורת שלה. לימים החלה החברה לספק פתרונות סנכרון לכל המפעילים הסלולריים והמפעילים הקוויים ושירתה את תחום הטלקום בכל הקשור לסנכרון תדר וזמן, היבט שיש לו חשיבות רבה בתחום התקשורת. במקביל למגזר הטלקום הרחיבה החברה את מגוון לקוחותיה והעניקה שירותי סנכרון ותזמון לחברות בתחום ה-בילינג, רשתות IT ורשתות פיננסיות, שם לתזמון יש משמעות קריטית. כיום פעילה החברה בארבעה תחומים עיקריים: טלקום, המגזר הביטחוני, לרבות פרויקטים לאומיים וביטחוניים קריטיים, המגזר הפיננסי ומגזר התשתיות הקריטיות והממשלתיות, כמו חברות האנרגיה, ורשתות ממשלתיות. ומעל לכל, פוקוס מסנכרנת ומתחזקת את המעבדה הלאומית לפיזיקה האחראית על הזמן הרשמי של מדינת ישראל.



עומר שורר | צילום: יח"צ

צילום: יח"צ מיקרוסמי