Secure – eTon
עלון בנושאי טכנולוגיות אבטחת מידע, יוצא לאור ע"י קומסק אבטחת מידע בע"מ
June 2001

דבר המערכת

שלום רב לכל קוראינו,
במהדורה הנוכחית של ה- Secur-eTon חדשות טריות בתחום אבטחת מידע, כתבה שניה בנושא PKI, ראיון עם מנהל אבטחת מידע בחברת בזק וסקירת תוכנת AppShield מבית סנקטום.
קריאה נעימה,
צוות העיתון וחברת קומסק-פבליקום

תוכן

עמוד 1 חדשות
עמוד 2 PKI - כתבה 2
עמוד 3 זרקור על מוצר
עמוד 3 סיפור לקוח

secureton@comsec.co.il

קרדיטים

כתיבה: רווית גרייצר, גיל פונדיק
ייעוץ טכנולוגי: שרון בסר
עריכה: אמיר קראוס

פרצת אבטחה בשרתי SQL של מיקרוסופט מאפשרת השתלטות

הפרצה קיימת רק בשרתים המקונפגים עבור זיהוי במוד משולב (Mixed Mode) Authentication

פרצת אבטחה בשרת ב- SQL Server 7.0 וב- SQL Server 2000 מאפשרת לפורצים להשתלט על שרתים אלה, כך טוענת מיקרוסופט בהודעה רשמית שפרסמה. החברה שחררה גם patch לתיקון הפרצה אותו ניתן להשיג ב: http://www.microsoft.com/technet/security/bulletin/MS01-032.asp

בעיה באופן שבו SQL מטפל בסיום חיבור לבסיס נתונים מאפשרת לפורצים להשתלט על חיבור של מנהל הרשת וכך לקבל את הפריבילגיות שלו. כאשר משתמש מסיים database session בשרת SQL, הקשר שזה עתה נסתיים נשמר באופן זמני ב- cache. ע"י שימוש בשאילתת שרת מסוימת, יכול התוקף לנצל זאת כדי לאתחל חיבור של מנהל רשת וכך לקבל את הפריבילגיות שלו. כך יכול הפורץ לעשות כל שינוי שעולה על דעתו בבסיס הנתונים, לרבות הוספה, שינוי או מחיקת מידע, ואף יכול באופן תיאורטי להריץ קוד על השרת על פי בחירתו.

יחד עם זאת, מיקרוסופט מדגישה שכדי לנצל את פרצת האבטחה הזו, השרת צריך להיות מקונפג לזיהוי במוד משולב, תהליך שבאמצעותו השרת מנסה לזהות משתמש באמצעות שיטות של Windows, ומשלא עולה הדבר בידו, מנסה לזהותו באמצעות בסיס הנתונים של שרת ה- SQL. באופציה זו נעשה בעיקר שימוש בשרתי SQL המריצים מערכות הפעלה Windows 95 ו- 98 ומיקרוסופט ידועה כמתנגדת נחרצות לתצורה זו. דבר נוסף המקשה על ניצול הפרצה הוא העובדה שהפורץ צריך לקבל קודם כל גישה לשרת כדי לאתחל חיבור מנותק.

צ'ק פוינט הוציאה את Service Pack 4 לגירסת 4.1

חברת צ'ק פוינט פרסמה השבוע את service pack 4 לתוכנת FW-1 / VPN-1 בגרסה 4.1 .

service pack זה מתקן מספר לקויים קודמים במוצר אשר יכלו אף לגרום לבעיות אבטחתיות (בעיקר בהקשר של Denial of Service). כמו כן כולל התיקון מספר רב של תוספות חשובות, לרבות:

1. זיהוי שרת Exchange על פי מאפייני תעבורה מדויקים ללא צורך בקיבוע פורטים ב- registry של שרת ה- Exchange . קודם לכן, פתיחת פורטים דינמיים ב- Exchange היתה נחסמת ע"י ה- firewall . כיום, ה- firewall יודע לזהות שמדובר בתעבורת Exchange ומאפשר תעבורת מידע גם בפורטים אלה.

2. תמיכה ב- **Persistent IPSec Tunnels.** באופן זה מתקצר משך הזמן הנדרש ליצירת VPN על ידי החלפת SA (Security-Association) עוד לפני שפג תוקפו של ה SA הנוכחי, גם אם לא נרשמה תעבורה במהלך אורך החיים של ה- SA הקודם. שינויים אלה משפרים את זמינות קישורי ה- VPN וביצועיהם.

COMSEC GROUP
Information Security

תשתית מפתחות ציבוריים (PKI): על הצפנות ודברים אחרים
(כתבה שניה בסדרה)

בגיליון הקודם הצגנו את המושגים העיקרים בנושא PKI, ובין היתר הזכרנו גם את נושא ההצפנה העומד בבסיס החלפת המפתחות. היום נעמוד על ההבדלים בין הצפנה סימטרית וא-סימטרית, חתימה דיגיטאלית, פונקצית ה- hash וננסה להבין על קצה המזלג איך עובדים דברים.

הצפנה היא תהליך שבו מידע הניתן לקריאה מומר לטקסט שאינו ניתן לקריאה ללא פענוח. הצפנה על צורותיה השונות קיימת מראשית ימי הכתב. ההיסטוריה רצופה בטכניקות הצפנה שונות כגון החלפת אותיות (alphabetic shift), שיטה שהונהגה עוד בימיו של יוליוס קיסר בה מוחלפות אותיות על פי סדר מסוים, דרך שימוש בשפות המדוברות ע"י כמות קטנה מאד של אנשים כגון השבט האינדיאני נבאהו (Navajo) וכלה בהצפנות ממוחשבות של ימינו אנו.

ניתן לחלק את ההצפנה לשתי שיטות עיקריות: הצפנה סימטרית והצפנה א-סימטרית.

הצפנה סימטרית משמעותה קידוד ופענוח ע"י מפתח שנקבע מראש. מפתח הוא למעשה מחרוזת מידע (אוסף של סיביות) אשר באמצעותו מבצעים פעולה על מידע המקור ומקבלים פלט שאינו ניתן להבנה ללא פענוח. בהצפנה סימטרית המידע מוצפן (ע"י השולח) ומפוענח (ע"י המקבל) באמצעות אותו המפתח. פרוטוקול ההצפנה הסימטרי המפורסם ביותר הנו Data Encryption Standard . DES הוא מנגנון הצפנה סימטרי שפותח בסוף שנות ה-70 ע"י IBM בחסות ממשלת ארה"ב. בשיטה זו משתמשים במפתח בן 56 סיביות, כלומר ישנם 2^56 מפתחות אפשריים . כיום קיימת הרחבה של האלגוריתם ל- Triple DES – כלומר הצפנה של 2^(3*56). הצפנה זו נחשבת לקשה יותר לפיצוח אך מסורבלת יחסית לשימוש ויקרה מבחינת צריכת משאביה. מחירה היקר נובע בעיקר מן העובדה שיש ליצור מספר רב של מפתחות לפחות כמספר האנשים שעימם קיים קשר המחייב הצפנה. בעיה נוספת קשורה לדרך הפצת המפתחות, בעיקר על פני תווך חשוף ולא מאובטח, כדוגמת האינטרנט.

הצפנה א-סימטרית מטרתה פענוח והצפנה ע"י הפעלת פעולות מתמטיות השונות זו מזו, דהיינו מפתחות שונים – מפתח ציבורי (public key) ומפתח פרטי (private key). המפתח הציבורי משמש להצפנת המידע וניתן להשיגו בקלות ב-directories (למשל כאלו המפורסמים על גבי האינטרנט) בעוד שהמפתח הפרטי המשמש לפענוח המידע, ידוע אך ורק לבעליו. המידע המוצפן בעזרת מפתח אחד, יכול להיות מפוענח אך ורק באמצעות המפתח השני (בן זוגו), ולא באמצעות שום מפתח אחר. כך לדוגמא, RSA היא שיטת ההצפנה הא-סימטרית הנפוצה ביותר כיום וקרויה על שם שלושת מפתחיה – Shamir -Adelman – Rivest (כן, יש שם גם מישהו משלנו). בבסיס השיטה עומדת הכפלה של 2 מספרים ראשוניים גדולים במיוחד כאשר המכפלה היא מרכיב גם במפתח הציבורי וגם במפתח הפרטי. כדי להבין את סדר הגודל של המספרים עליהם מדובר, ניקח את דוגמת הבנקים שמכפלות המספרים הראשוניים בדרך ליצירת המפתחות שלהם מגיע כיום ל-10^308. לו כל המחשבים הביתיים שבעולם (לערך רבע מיליארד) היו מתגייסים למשימת הפיצוח, התהליך היה אורך למעלה מגילו של היקום.

לצורך המחשה, ניקח למשל שיח' סעודי המבקש להעביר 2 מיליארד דולר מבנק בריאד לבנק בציריך. לשם כך, הוא שולח הודעה מוצפנת הכוללת את פרטי חשבונו ופרטים אישיים נוספים ומצפין אותה באמצעות המפתח הציבורי של הבנק הידוע לכל. הבנק מפענח את ההודעה באמצעות מפתחו הפרטי.

Hashing. אולם השיח' רוצה להיות בטוח מעל לכל ספק שלא אונה להודעתו כל רע ושלא עברה שינויים בדרך (message integrity) ולשם כך הוא מוסיף hashing למסמך, פעולה מתמטית חד כיוונית שבסופה מתקבל ערך מתמטי מסוים המייצג את המסמך (משום כך התהליך נקרא גם message digest , כלומר תקציר ההודעה); המקבל (במקרה זה הבנק) יבצע את אותה הפעולה על המסך המקורי (לאחר פענוח) וישווה את התוצאה שקיבל לערך ה- hash שנשלח אליו. שינוי בערכי ה- hash ולו הקטן ביותר יעיד על כך שהיתה פגיעה באותנטיות של המסר. פעולת ה- hashing היא פעולה חד-כיוונית במובן זה שניתן אמנם להפיק ערך hash מההודעה אולם אין דרך ידועה לחזור להודעה מהערך שהתקבל.

חתימה דיגיטאלית. נותר עוד ענין "פעוט": כיצד יוכל כעת הבנק לאמת את זהות השולח ולדעת שזהו אכן השיח'? התשובה היא חתימה דיגיטאלית, תוספת אלקטרונית (דיגיטאלית) המצורפת למידע טרם שליחתו המאפשרת את זיהויו של השולח. השיח למעשה חותם את "תקציר המסמך" (hash value) באמצעות מפתחו הפרטי וכך ניתן לפתוח אותה באמצעות מפתחו הציבורי ולדעת שאכן מדובר בשיח.

* יש לציין שדוגמת השיח' היא דוגמא אחת מיני רבות ממגוון הרחב של אפשרויות שמקנה השימוש בתשתית PKI. באופן עקרוני, ניתן להצפין ולחתום, רק להוסיף חתימה דיגיטאלית מבלי להצפין ועוד כהנה וכהנה אולם מפאת חוסר מקום הסתפקנו בדוגמא אחת.

זרקור על מוצר

Sanctum AppShield

מחקרים רבים מראים שהשימוש באמצעי אבטחה סטנדרטים (Firewall לרמת הרשת ו-SSL להצפנה של הנתונים), פגיע לחלוטין לפרצות ברמת האפליקציה ומותיר את מסדי הנתונים ותפקוד האתר חשופים לפורצים.

חברת סנקטום (לשעבר Perfecto Technologies), חברה ישראלית שנוסדה בשנת 1997 וחלוצה בתחום אבטחת אפליקציות, פיתחה את AppShield , תוכנה שנועדה להגן על אתרי e-Business ברמה האפליקטיבית. AppShield מותקנת על גבי שרתי אינטרנט ומתנהגת כמו proxy הבודק את כל הבקשות. באמצעות שימוש במנוע זיהוי מדיניות ((Policy Recognition Engine, AppShield מנתחת כל דף אינטרנט יוצא ולומדת את מדיניות האבטחה שלו תוך כדי תנועה. הדפים המוחזרים מושווים למדיניות כדי לוודא שלא נעשו שינויים בדפים אלה. התוכנה מזהה מייד כל שינוי וחוסמת באופן אוטומטי כל בקשה לא חוקית, מתעדת אותה בלוג ושולחת התרעה הן למנהל הרשת והן לתוקף על כך שפעילותו תועדה.

כתוצאה מכך נמנעת גישה בלתי חוקית למידע ולקבצים באמצעות אפליקציות אינטרנט

השימוש ב- AppShield מצריך מעט ידע נוסף באפליקציות אינטרנט שכן אמנם התוכנה לומדת בעצמה את מדיניות האבטחה של האפליקציה, אולם שינויים הנעשים באפליקציות מחייבים שינויי קונפיגורציה ב- AppShield . התוצאה הסופית היא שלפורצים אין שום דרך לגשת באופן בלתי חוקי למידע ולקבצים באמצעות אפליקציות אינטרנט.

features נוספים כוללים תמיכה בכלי ניהול מרכזיים כגון Tivoli ו-HP OpenView, תמיכה באתרים מוצפני SSL ולאחרונה אף קיבלה AppShield אישור OPSEC של חברת צ'ק פוינט, דבר המבטיח תאימות ועבודת רשת שיתופית עם VPN-1/FireWall-1 של צ'ק פוינט.

סיפור לקוח

שוחחנו עם מר חיים פלדמן, מנהל אבטחת מידע בחברת בזק, על מערך אבטחת המידע בחברה ועל פעילות חברת קומסק בבזק.

מהי רמת המודעות לאבטחת מידע בבזק?

נושא אבטחת מידע בחברת בזק מצוי תחת אחריות אגף הביטחון, מחלקת אבטחת מערכות מחשוב ותקשורת. זוהי למעשה מחלקה נפרדת מיחידות המחשוב השונות בחברה על מנת להבטיח שההחלטות שיתקבלו והפעילויות שינקטו בנושא אבטחת המידע יהיו אובייקטיביות לחלוטין. נושא אבטחת מידע בבזק תפס תאוצה לפני מספר שנים ובתור צעד ראשון הוחלט לערוך סקר סיכונים מקיף שתפקידו למפות את כל המערכות הארגוניות ולהתריע בפני חשיפות אבטחה קיימות.

ואז קומסק נכנסה לתמונה?

כן, פרסמנו מכרז בו גברה קומסק על מספר מתחרות ואז החלה העבודה על הסקר שנמשכה קרוב לשנה. במסגרת סקר הסיכונים עסקה קומסק במיפוי המערכות השונות, באיתור מאגרי מידע, עדכון הנהלים וכד' .

מה נעשה במסגרת הסקר?

קומסק ערכה מיפוי למערכות השונות בחברה במטרה למצוא חשיפות פוטנציאליות, עדכנה את נהלי אבטחת המידע שנמצאים כיום על גבי אתר האינטראנט של בזק, איתרה את מאגרי מידע החייבים ברישום על פי החוק במשרד המשפטים וכן עזרה בגיבוש תוכנית עבודה שנתית בנושא אבטחת מידע על סמך ממצאי הסקר.

בעקבות הסקר וגיבוש מדיניות אבטחת המידע לארגון הוחלט גם על הקמת ועדת היגוי ליישום מדיניות אבטחת מידע בחברה שחברים בה שלושת הסמנכ"לים הרלוונטים, מנהלי אגפי הטכנולוגיה ובעלי התפקידים השונים שמנהלים את נושא אבטחת המידע בארגון.

מהן תוכניותיה של בזק בנושא אבטחת מידע?

ניתן בעצם לסווג את תוכניות בזק לתוכניות לטווח הקצר ולתוכניות לטווח הארוך. בטווח הקצר (בשנה הקרובה), אנחנו מתכננים להכניס מערכת לניהול מרכזי של משתמשים המבוססת על פרופילי משתמשים. כמו כן, אנחנו מצויים כרגע בתהליך של הרצה למערכת Provider-1 של צ'קפוינט לניהול מרכזי של מערכות Firewall , נתבים ורכיבי אבטחה אחרים. גם נושא ה-PKI והזדהות באמצעים חכמים נמצא כרגע בשלבי ניסוי ואנחנו מקווים שגם הנושא הזה יתפוס תאוצה בשנה קרובה. מאוחר יותר, בכוונתינו להכניס מערכת שליטה ובקרה שתקבל דיווחים מכל המערכות, להכניס אמצעי זיהוי ביומטריים ועוד.

*למען הסדר הטוב, מר פלדמן ביקש להוסיף שגם חברות אבטחת מידע אחרות כגון אקספרט ואדאנט נמצאות בקשרי עבודה עם בזק.