בדיקת חדירה מוכיחה שפרצת אבטחת הסייבר של Torvik Industries על-ידי "הזאב" יכולה הייתה להימנע באמצעות המדפסות של HP

דוח סיכום רשמי עבור הפריצה לנתונים

מגזר עסקי
משלוח

מטרה
ניתוח ופתרון תחומים שבהם קיימת נקודת תורפה של הרשת

גישה
בדיקת חדירה לאיתור נקודות התורפה שהובילו להתקפה

ממצאים והמלצות
- לימוד משתמשים להיות חשדניים לגבי פתיחת הודעות דוא"ל חשודות וקבצים חשודים המצורפים להדפסה
- פריסת מדפסות HP עם זיהוי אימים
- הגדרת התצורה של כל נקודות הקצה עבור אבטחה, כולל תשתית שהועברה או נמצאת במיקום זמני

העסק קובע
יישום אמצעי אבטחה חזקים יותר כדי להימנע מזמן השבתה תפעולי וכדי לשפר את הביטחון במותג. שיפור מדיניות לניטור נקודות קצה של רשת במיקומים זמניים.

סקירה

Torvik Industries* שולחת 8 מיליון מכולות מדי שנה. עבור 22,000 יצרנים וסיטונאים, Torvik היא הקשר החיוני שבין המוצרים והאנשים בכל רחבי העולם. נכסי החברה כוללים מספנות, כלי שיט, מחסנים ואת כל הטכנולוגיה התומכת ברשת הנרחבת של Torvik.

כאשר החברה גדלה, תשתית הטכנולוגיה שלה נאבקה כדי להתאים את עצמה. בעוד שצוות אבטחת ה-IT קבע את תצורת שרתי החברה, חלק מהמדפסות במשרדים נלווים או במיקומים זמניים אינן מנוהלות מבחינת האבטחה.

ב-23 באפריל 2018, פושע הסייבר המוכר רק כ-"The Wolf" (הזאב) השתמש במדפסת לא מאובטחת כדי לחבל בפעולותיה של Torvik Industries, החל ממחשבים אישיים, דרך עגורנים וכלה באוניות מכולה. יועץ האבטחה שלהם השתמש בבדיקת חדירה כדי לנתח את האירוע וסיפק המלצות להגדלת האבטחה ולהכשרת הצוות.

מה קרה

הנהלת Torvik Industries נהגה להיות זו שמחליטה במקרים הכרוכים בסיכון גבוה - ולכן הם לא ציפו שפורצי מחשבים יחדרו לרשת שלהם בצורה כה עמוקה שתשבית את עגורני העמוד של החברה ותשנה את הכיוון של ספינות באוקיינוס הפתוח.

כל מה שהזאב היה צריך לעשות זה לפגוע במדפסת לפורמט גדול באתר בנייה. לאחר מכן הוא הצליח להתקדם בצורה רוחבית דרך רשת החברה אל היעדים הגדולים בתפעול החברה. תוך רגע, חברת הובלה ימית מובילה זו ניצבה בפני הפרעות תפעוליות עצומות, גינוי בינלאומי רחב ואלפי לקוחות זועמים.

איך זה קרה

צוות אבטחת ה-IT של החברה חשב שהחברה מוגנת. הצוותים הטכנולוגיים והלוגיסטיים שלה ניטרו באופן קבוע את הפעולות הגלובליות לאיתור בעיות אבטחה אפשריות. בחברה היו אפילו נוהלי אבטחה בשימוש עבור נקודות קצה כגון מדפסות. אבל הם התעלמו ממשהו: תצורת האבטחה של המדפסת לפורמט גדול הייתה ממוקמת זמנית בקרון באתר בנייה.

פורץ המחשבים אפילו לא היה צריך לגשת למדפסת ישירות - הוא פשוט שלח הודעת דוא"ל עם קובץ מצורף בתבנית PDF אל עובד Torvik האחראי להדפסת מסמכים בפורמט גדול. PDF זה כלל קובץ Postscript נסתר ששימש ככלי נשק ויכול היה לפתוח ולהפעיל את עצמו כאשר ה-PDF נשלח למדפסת. כאשר העובד שלח את עבודת ההדפסה, התוכנה הזדונית שיבצה את עצמה במדפסת והתפשטה בכל רחבי הרשת. על-ידי הוספת תוכנה זדונית לקובץ מצורף לדוא"ל התמים למראה, פורץ המחשבים עקף את התוכנה למניעת תוכנות זדוניות במחשבי החברה.

הפרצה הייתה אפשרית משום שלמדפסת בפורמט הגדול לא הייתה אבטחה מובנית חזקה, כגון זיהוי אימים. בנוסף, החברה לא הצליחה לנטר ולנהל את התצורה של כל מדפסת יחידה בצי המדפסות - כגון אלה המוצבות זמנית במשרדים נלווים.

תיקון הפרצה

Torvik Industries שכרה חברה מובילה לבדיקת חדירה לביצוע ניתוח מקיף של אבטחת הסייבר של הארגון.

צוות בדיקת החדירה המליץ להתקין מדפסות HP בעלות מאפייני אבטחה משובצת, כולל את סדרת HP DesignJet עם אתחול מאובטח ויצירת רשימות לבנות של קושחה. מאפיינים אלה מסייעים למדפסת לזהות קוד זדוני ולכבות את עצמה, ולאחר מכן לשלוח התראה ל-IT לגבי הצורך בהתקנה מחדש של קושחת HP חוקית.

הם המליצו גם להשתמש במאפיין האבטחה Instant-On של HP JetAdvantage Security Manager, תוכנה לניהול אבטחה בכל רחבי צי המדפסות, כדי להחיל אוטומטית מדיניות אבטחה ברגע שהתקנים מתווספים לרשת. HP Security Manager יכול גם ליצור דוחות תאימות המציגים כל מדפסת HP, גם במיקומים מרוחקים או זמניים. זה עוזר להדגים את תצורות אבטחת הצי שנשמרו.

בנוסף, יועץ האבטחה הציע תוכנית הוראה שתעזור לעובדים לזהות הודעות דוא"ל חשודות ותמנע הדפסת קבצים מצורפים לא ידועים.

סוף דבר

Torvik Industries עדיין מתאוששת מההשפעות של פרצת אבטחת הסייבר בתפעול שלה, וכן מהפרסום המודגש שזכו לו ההשקפות הלא קונבנציונליות והפעולות הפליליות של הנשיא שלה. בעוד שהארגון מנסה לפתח כיוון חדש מבחינת הנהגה, כיוון אבטחת הסייבר ברור: שימוש במדפסות ובפתרונות של HP יסייע בעצירת הזאב הבא שייצא לצוד.

**Torvik Industries היא חברה בדויה ששימשה כמטרה להתקפת סייבר גדולה בסרט של HP Studio, "THE WOLF: אלפא אמיתי".*

לקבלת מידע נוסף על פתרונות HP:
HP DesignJet: hp.com/go/designjetsecurity
אבטחת הדפסה: hp.com/go/reinventsecurity

כדי לצפות בסרטי "The Wolf", בקר בכתובת:
hp.com/thewolf

הירשם לקבלת עדכונים
hp.com/go/getupdated

שתף עם עמיתיך

4AA7-3562HEE, אוגוסט 2018