



עלון המודעות החודשי לביטחון עבורך

שימוש מאובטח בענן

סקירה כללית

אולי שמעתם על המושג שנקרא "הענן". המשמעות היא שימוש בספק שירות באינטרנט לאחסון וניהול הנתונים שלך. דוגמאות כוללות יצירת מסמכים ב-Google Docs, גישה לדוא"ל ב-Microsoft 365, שיתוף קבצים באמצעות Dropbox או אחסון התמונות שלך ב-iCloud של אפל. בזמן שאתה ניגש ומסנכרן את הנתונים שלך ממספר מכשירים בכל מקום בעולם ומשתף את המידע שלך עם כל מי שאתה רוצה, לעתים קרובות אינך יודע ולא יכול לשלוט היכן הנתונים שלך מאוחסנים פיזית.

בחירת ספק ענן

שירותי ענן אינם טובים ואינם רעים. הם כלים לביצוע דברים. עם זאת, כשאתה משתמש בשירותים אלה, אתה בעצם מעביר את הנתונים הפרטיים שלך לזרים, ומצפה שהם ישמרו גם מאובטחים וגם זמינים. ככזה, אתה רוצה להיות בטוח שאתה בוחר את ספק השירות שלך בחוכמה. לקבלת מידע הקשור לעבודה, בדוק עם המנהל שלך אם אתה רשאי להשתמש בשירותי ענן ואילו מהם מורשים. אם אתה שוקל להשתמש בשירותי ענן לשימוש אישי, שקול את הדברים הבאים:

1. **אמון:** האם אתה יכול לסמוך על ספק הענן? האם מדובר בחברה ציבורית ידועה שמיליוני אנשים כבר משתמשים בה, או שמדובר בחברה קטנה ובלתי ידועה שמבוססת במדינה שמעולם לא שמעתם עליה?
2. **תמיכה:** כמה קל לקבל עזרה או לקבל תשובה לשאלה? האם יש מספר טלפון שאליו אתה יכול להתקשר או כתובת דוא"ל שאליה תוכל ליצור קשר? האם יש אפשרויות אחרות לתמיכה, כגון פורומים ציבוריים או שאלות נפוצות באתר שלהם?
3. **פשטות:** כמה קל להשתמש בשירות? ככל שהשירות מורכב יותר, כך גדל הסיכוי שתעשה טעויות ותחשוף או תאבד בטעות את המידע שלך. השתמש בספק ענן שקל להבין, להגדיר ולהשתמש בו קל.
4. **אבטחה:** איך הנתונים שלך יגיעו מהמחשב שלך לשירות הענן? האם החיבור מאובטח באמצעות הצפנה? כיצד נשמרים הנתונים שלך? האם הם מוצפנים, ואם כן, מי יכול לפענן את הנתונים שלך? כשאתה מעביר את הנתונים שלך, זכור שאבטחה היא אחריות משותפת בינך לבין הספק.
5. **תאימות:** האם ספק השירות תומך בכל המכשירים ומערכות ההפעלה שבהם אתה משתמש או מתכנן להשתמש?
6. **תנאי שירות:** הקדש רגע לעיון בתנאי השירות (לעתים קרובות הם קלים להפליא לקריאה). על פי חוקים של איזו מדינה פועל ספק השירות? שים לב במיוחד לזכויות שאתה נותן לספק השירות שלך.

אבטחת הנתונים שלך

השלב הבא הוא לוודא שאתה משתמש בשירותי הענן שלך כראוי. אופן הגישה והשיתוף של הנתונים שלך יכול לעתים קרובות להשפיע הרבה יותר על אבטחת הנתונים שלך מכל דבר אחר. כמה צעדים מרכזיים שתוכל לנקוט כוללים:

1. **אימות:** השתמש בסיסמה חזקה וייחודית כדי להגן על חשבון הענן שלך. אם ספק הענן שלך מציע אימות דו-שלבי, אנו ממליצים בחום להפעיל אותו.
2. **שיתוף קבצים / תיקיות:** ספקי ענן מקלים מאוד על שיתוף נתונים - לפעמים פשוט מדי. יכול להיות קל מאוד לשתף בטעות את המידע שלך בפומבי. הגן על עצמך על ידי מתן גישה לאנשים ספציפיים (או קבוצות אנשים) רק לקבצים או תיקיות ספציפיים. כשמישהו כבר לא זקוק לגישה, הסר אותו. ספק הענן שלך אמור לספק דרך קלה לעקוב אחר מי שיש לו גישה לקבצים ולתיקיות שלך.
3. **הגדרות:** הבן את הגדרות האבטחה שמציע ספק הענן שלך. לדוגמה, אם אתה משתף תמונות, קבצים או תיקיה עם מישהו אחר, האם הם יכולים לשתף את הנתונים שלך עם אחרים ללא ידיעתך?
4. **חידוש:** אל תשכח לחדש את המנוי שלך, אחרת אתה עלול לאבד את הגישה לנתונים שלך.

עורכת אורחת

טמייקה ריד (@womeninlinux), מייסדת נשים בלינוקס. היא מובילה יוזמות תוך התמקדות בחקר קריירה בתשתיות, אבטחת סייבר, DevSecOps ומנהיגות. היא מארחת מפגש שבועי עם נשאים הנעים בין תשתיות לבלוקצ'יין. היא דיברה ב- OSCon, LISA, Seagl ו- HashiConf האיחוד האירופי.

משאבים

הנדסה חברתית: <https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering>
סיסמאות: <https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Hebrew.pdf>
מנהלי סיסמאות: <https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Hebrew.pdf>
כוחו של עדכון: <https://www.sans.org/security-awareness-training/resources/power-updating>

תורגם לקהילה על ידי: גדי מרגלית ודורון ענבר

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Awareness Security, הפצתו ברישיון [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). הנך רשאי להפיץ או להשתמש בעלון זה, כל עוד אתה לא מוכר או מבצע שינויים בעלון זה. עורכי המערכת: וולט סקריבנס, פיל הופמן, אלן וגובר, לס רידוט, פרינסס יאנג.