אאוץ! | בנובמבר 2016

מרכז סליקה בנקאי בע"מ שירותי בנק אוטומטיים בע"מ

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- סקירה כללית
- בחירת ספק ענן
- אבטחת הנתונים שלך

שימוש בענן מאובטח

סקירה כללית

משמעות "הענן" יכולה להיות שונה לאנשים שונים, אבל בדרך כלל זה אומר להשתמש בספק שירותים באינטרנט כדי לאחסן ולנהל את מערכות המחשוב שלך ו / או הנתונים שלך. אחד יתרונות של הענן הוא שאתה יכול לגשת בקלות ולסנכרן את הנתונים שלך ממספר התקנים בכל מקום בעולם, אתה יכול גם לשתף את המידע שלך עם מי שאתה רוצה. אנו קוראים לשירותים אלו "הענן" כי לעיתים קרובות אתה לא יודע איפה הנתונים שלך מאוחסנים פיזית. דוגמאות של מחשוב ענן כוללים יצירת מסמכים בגוגל מסמכים, שיתוף קבצים באמצעות Dropbox, הגדרת שרת משלך בענן אמזון, אחסון נתוני לקוחות ב- Salesforce, שמירת מוסיקה או תמונות בארכיון של אפל - iCloud. שירותים מקוונים אלו יכולים לגרום לך להיות הרבה יותר פרודוקטיבי, אבל הם גם באים עם סיכונים ייחודיים. בניוזלטר זה אנו מכסים איך אתה יכול בבטחה להפיק את המיטב מהענן.

עורך אורח

דייב Shackleford (**@daveshackleford**) יועץ מקצועי בעל חברת האבטחה "וודו" והמחבר של קורסי הכשרת SANS רבים, כולל קורס אבטחה SANS מספר 579: אבטחת וירטואליזציה, וענן פרטי, קורס מספר 524: יסודות האבטחה.

בחירת ספק ענן

הענן הוא לא טוב ולא רע, הוא כלי שמטרתו הוא לעשות את מה שאנחנו רוצים, הן בעבודה והן בבית. עם זאת, כאשר אתה משתמש בשירותים אלו אתה מוסר את מידע פרטי שלך לאחרים ואתה מצפה מהם לשמור אותו מאובטח וז־מין. עקב כך, אתה רוצה להיות בטוח שאתה בוחר את ספק הענן שלך בחוכמה. עבור מחשבי עבודה או מידע בנושא עבודה, עלייך לבדוק עם הממונה שלך בכדי לראות האם החברה מאפשרת לך להשתמש בשירותי ענן. אם מותר לך להשתמש ענן, תוודא באיזה שירותי ענן אתה יכול להשתמש ומה המדיניות של אופן השימוש בה. אם אתה שוקל שירות ענן לשימוש האישי שלך, שקול את הנקודות הבאות.

1. **תמיכה** - עד כמה פשוט לקבל עזרה או מענה לשאלתך? האם יש כתובת דוא"ל שתוכל ליצור קשר, פורומים ציבוריים שתוכל לפרסם שאלות או לבדוק את אתר האינטרנט שלהם לשאלות נפוצות.

שימוש בענן מאובטח

2. **פשטות** - כמה קל להשתמש בשירות? ככל שהשירות מורכב יותר, כך גדל הסיכוי שאתה תעשה טעויות, לדוגמא לחשוף בטעות את המידע שלך או לאבד אותו בחר ספק ענן אשר קל לך להבין את ההגדרות שלו וצורת השימוש.
3. **אבטחה** - איזה נתונים נאספים אודותיך, אם בכלל? איך הנתונים שלך מועברים מהמחשב אל הענן וכיצד הוא מאוחסן בענן – האם המידע מוצפן? ואם כן מי יכול לפענח את הנתונים שלך?
4. **תנאים והגבלות** - קחו רגע כדי לבדוק את תנאי השירות (הם לעתים קרובות מפתיעים בקלות לקריאה). תוודא שאתה שיכול לגשת לנתונים שלך ומה הזכויות המשפטיות שלך, תבדוק את האחריות מבחינת אבטחה מצד הספק או מה נדרש על ידך.

הענן יכול להפוך את המידע שלך לנגיש יותר ולעזור לך להיות יותר פרודוקטיבי, אבל יש להיזהר כיצד אתה מנגיש ומשתף את המידע שלך.

אבטחת הנתונים שלך

לאחר שבחרת ספקית ענן, הצעד הבא הוא לוודא שאתה משתמש בשירותי הענן שלך כמו שצריך. איך אתה ניגש ומשתף את הנתונים שלך, לעתים קרובות יש השפעה גדולה על אבטחת הקבצים שלך. כמה שלבים עיקריים שניתן לנקוט:

1. **אימות** - השתמש בביטוי סיסמא חזק וייחודי על מנת לבצע אימות לחשבון הענן שלך. אם ספק הענן שלך מציע אימות דו-שלבי אנו ממליצים בחום להפעיל אותו. זהו אחד הצעדים החשובים ביותר שאתה יכול לנקוט כדי להגן על החשבון שלך.
2. **שיתוף קבצים / תיקיות** - הענן עושה את השיתוף מאוד פשוט, לפעמים יותר מדי פשוט. בתרחיש הגרוע ביותר, אתה עלול לחשוב שאתה משתף את הקבצים שלכם עם רק אדם ספציפי, אבל אתה יכול בטעות להפוך את הקבצים או אפילו תיקיות שלמות זמינות לציבור האינטרנט כולו. הדרך הטובה ביותר להגן על עצמך היא לא לשתף את כל הקבצים שלכם עם מישהו אחר כברירת מחדל. אז רק לאפשר לאנשים ספציפיים (או קבוצות של אנשים) גישה לקבצים או תיקיות ספציפיים על בסיס הצורך לדעת. כשמישהו כבר לא צריך גישה לקבצים שלך, להסיר אותם. ספק הענן שלך צריך לספק לך דרך קלה לעקוב אחרי מי שיש לו גישה לקבצים והתיקיות.
3. **שיתוף קבצים / תיקיות בעזרת קישורים** - תכונה משותפת אחת לכמה חברות של שירותי ענן היא היכולת ליצור קישור לאינטרנט אשר מצביע על הקבצים או התיקיות. תכונה זו מאפשרת לך לשתף את הקבצים הללו עם

שימוש בענן מאובטח

כל מי שתרצה פשוט על ידי מתן קישור אינטרנט. עם זאת גישה זו מסוכנת מבחינת אבטחה, מישהו שיודע על קישור זה עשוי לקבל גישה לקבצים או לתיקיות אישיות שלך. אם אתה שולח את הקישור רק לאדם אחד, אדם זה יכול לשתף את הקישור עם אחרים או לשתפו כך שהמידע יופיע במנועי חיפוש. אם אתה משתף נתונים באמצעות קישור, כדאי להיות בטוח שאתה יכול להשבית את הקישור כאשר הצד השני כבר לא צריך את הקבצים אם זה אפשרי על ידי הגדרת תאריך תפוגה או, הגן על הקישור באמצעות סיסמא.

4. **הגדרות** – דאג להבין את הגדרות האבטחה המוצעות על ידי ספק הענן שלך. לדוגמה, אם אתה משתף תיקיה עם גורמים אחרים האם הם יכולים בתורם לשתף את הנתונים שלך עם גורמים נוספים ללא ידיעתך? בדוק האם יש דרכים לראות מי צפה בתוכן המשותף שלך. אתה יכול להגביל את השיתוף "לקריאה בלבד" לעומת "קריאה + כתיבה", כלומר אנשים יכולים גם לשנות את הקבצים שלך.
5. **אנטי וירוס** - ודא כי יש לך את הגרסה האחרונה של תוכנת האנטי וירוס המותקנת במחשב שלך ועל כל מחשב אחר אשר משתף את הנתונים שלך. אם קובץ שאתה משתף או מקבל נגוע, מחשבים אחרים יוכלו לגשת לאותו קובץ ולהידבק.

למד עוד

הרשם לעלון OUCH! המפורסם אחת לחודש, עלון זה מתמקד במודעות אבטחת המידע, ניתן לקרוא עלונים קודמים וניתן ללמוד על מודעות אבטחת המידע של SANS באתר securingthehuman.sans.org/ouch/archives.

מקורות

אימות בשני שלבים:	https://securingthehuman.sans.org/ouch/2015#september2015
ביטוי סיסמה:	https://securingthehuman.sans.org/ouch/2015#april2015
מנהל סיסמאות:	https://securingthehuman.sans.org/ouch/2015#october2015
מהי תוכנה זדונית:	https://securingthehuman.sans.org/ouch/2016#march2016
מאמר 524 אבטחת הענן:	https://sans.org/sec524

עורכי המערכת: ביל ויימן, וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי
תורגם על ידי: גדי מרגלית ודרור ענבר

