Newsletter

לקוחות יקרים!

איומיי סייבר ואבטחת מידע אינם תופעה חדשה, אולם מגיפת הקורונה הביאה עמה באופן ברור לעליית מדרגה בתחום ההונאות, ניסיונות גניבת מידע וזהות, פישינג, פריצות על רקע לאומני, השחטת אתרים, התקפות DDOS (Denial of service), כופר ואף התקפות על תשתיות לאומיות.
בעקבות מקרים חמורים שאירעו בעת האחרונה לעסקים בישראל, ובהיותנו אחד משחקני ה-Hosting & Cloud provider הגדולים בישראל, מצאנו לנכון להוציא מספר המלצות ופעולות הכרחיות למניעת פריצות לאתרים של לקוחותינו.

רקע כללי

רוב מתקפות הפריצה נעשות בעזרת כלים אוטומטיים או "רובוטים", שפשוט מחפשים נקודות כניסה "רכות" הנמצאות בהרבה אתרים שנבנו ללא מחשבה על סדרי אבטחה. ניסיונות פריצה אלו אינם מתוכננים לפגוע באדם או גוף כזה או אחר. אלו הן סריקות אוטומטיות שמנסות לפרוץ לכל גורם הנמצא ברשת ללא אבחנה מי הוא הגוף (כתבנו מסמך זה דווקא מסיבה של מתקפות ייעודיות על ישראל, אבל גם אם ממקדים את סריקות החולשה על ישראל, ראשון נפרץ מי שסידורי האבטחה שלו דלים).
ישנם מקרים שבהם כוונת הפורצים היא לפרוץ לגוף מסוים, אך זה קורה לרוב מסיבות של תחרות, נקמה או על רקע לאומני.

סיסמאות

לא ניתן להמעיט בגודל החשיבות של סיסמה מאובטחת, מכיוון שזהו המנגנון הראשון שפוגש הפורץ. אנו מדברים על סיסמה לניהול האתר, למשתמשים באתר או לתיבות דואר (נרחיב בהמשך) וכן לחיבור למסד הנתונים. על הסיסמה להכיל את התנאים הבאים:

- סיסמה בת 10 תווים לפחות (ומומלץ אף יותר)
- סיסמה הכוללת אותיות קטנות וגדולות (באנגלית)
- סיסמה שיש בה תווים מיוחדים כגון: $ % # @ !
- הסיסמה לא תכיל את שם המשתמש בתוכה או את שם האתר
- מומלץ שלכל ממשק שדורש סיסמה תהיה סיסמה שונה
- מחשש שלא תזכרו את הסיסמאות ניתן להשתמש במנהל סיסמאות (ראו לינק)
- יש להחליף סיסמה בתדירות גבוהה

לינקים:
1. ניתן להפיק סיסמאות חזקות העומדות בקריטריונים באמצעות האתר הבא: https://passwordsgenerator.net/
2. אחד משומרי הסיסמאות שניתן להיעזר בו: https://www.lastpass.com/password-manager

עדכונים

רוב אתרי הקוד הפתוח כיום בנויים בפלטפורמת WordPress או בממשקים לבניית תוכן הנקראים בשם כולל CMS. אותם ממשקים כוללים בתוכם תוספים (פלאגינים), תבניות וקבצי בסיס. האבטחה של האתרים הנ"ל תלויה בניהול נכון שלהם ובמעקב. לכן חשוב מאד לתת דגש על בדיקה שבועית או דו שבועית של עדכונים, עדכוני פלאגין, עדכוני תבנית ועדכוני הממשק עצמו.
המשחק בין הפורצים לנותני השירות הוא משחק של חתול ועכבר, וכשהפורץ מוצא פרצת אבטחה בקוד, מיד נותני השירות מוציאים עדכון עם סתימת הפירצה. **אם לא תעדכנו אתם בוודאי תיפרצו, זה רק עניין של זמן ומזל!**
בשרתי פלסק ישנו מנגנון עדכון אוטומטי בתוך אפליקציית ניהול לוורדפרס הנקראת WordPress Toolkit –

ומאוד מומלץ להפעילו!

אימות ב-2 שלבים

חיסמו את האתר והפאנל שלכם (C-Panel / Plesk) בעזרת אימות משולב בעת ההתחברות. באופן זה, גם אם פורץ ישיג את הסיסמה שלכם, עדיין כדי להתחבר יהיה עליו לקבל אישור מהטלפון או המייל שלכם להיכנס לאתר או לשרת. כך גם תדעו על כל ניסיון כניסה של כל מי שיינסה להיכנס לניהול האתר או לשרת שלכם.

לינקים:
1. עבור וורדפרס ניתן להתקין ולהגדיר את הפלאגין הבא: https://wordpress.org/plugins/wp-2fa/
2. עבור פלסק ישנו מגוון של פתרונות הנוגעים לאימות ב2 שלבים. לדוגמא:
   https://www.plesk.com/extensions/ldap-auth/
   כמו כן אפשר להשתמש בגוגל בלינק הנ"ל: https://www.plesk.com/extensions/google-authenticator/

חשבון מייל – E Mail

כל מה שכתבנו לגבי סיסמאות לאתר נכון גם לגבי חשבון הדוא"ל. יש לדעת שדואר אלקטרוני הוא אחת מנקודות החולשה הנפוצות ביותר שקיימות. לכן יש ליישם את ההנחיות הבאות:

- לקיים פוליסת סיסמאות כמו שנאמר בפרק הסיסמאות – הכי חשוב!
- כדאי ליצור תיבות דואר עם שמות לא שגרתיים, ולא להשתמש בתיבות דואר נפוצות כמו info או sales, גם אם זה יותר נוח, כי שמות כאלה מועדים לפריצות.
- להגדיר אנטי וירוס **על כל מחשב** שממנו נכנסים לעדכן את האתר או את מערכות הניהול. הרבה פעמים פריצות מתבצעות דווקא ממחשב ביתי שהוא פחות מוקשח ומאובטח.
- אין להעביר את הסיסמה לאף אחד, ואם כבר מעבירים אז מומלץ לשנות אותה מיד לאחר מכן.

שרתים ייעודיים / Cloud

בשרתים ייעודיים ניתן למצוא מנגנוני אבטחה רבים וחשובים, אך יש להקפיד על מספר כללים פשוטים שימנעו את רוב הבעיות:

- עדכוני מערכת הפעלה – LINUX \ WINDOWS
- עדכוני פאנל ניהול – PLESK \ CPANEL
- סיסמאות מורכבות העומדות בתנאים שרשמנו בפרק הסיסמאות
- Firewall חיצוני או פנימי (בהתאם לצורך) **פעיל**
- חסימת מדינות שאין צורך לתעבורה מהן, בדגש על מדינות עוינות, ע"י Firewall
- התקנת רכיב אבטחה MODSECURITY עם מנגנון הגנה חכם כגון ATOMIC (ראו לינק)
- VPN – במידת האפשר כדאי ומומלץ לאפשר גישת מנהל לשרת רק ע"י הצפנה
- הפעלת מנגנון חסימה fail2ban בשרתי LINUX למי שנכשל מספר פעמים בכניסה לשרת – fail2ban (ראו לינק)
- Windows – שינוי פורט לגישה מרוחקת (RDP)

לינקים:
1. מסנן חשוב למוד סקיוריטי: https://www.plesk.com/extensions/offer-adv-modsecurity-rules/
2. Fail2ban – עבור לינוקס: https://support.plesk.com/hc/en-us/articles/213956105-How-to-install-fail2ban-on-Plesk-for-Linux

הסתרת כתובת האתר והגנה נוספת

אחת מהאסטרטגיות האפשריות למניעת פריצה היא שימוש בחברות צד שלישי המנהלות את התעבורה המגיעה לשרת ומסתירות את כתובת השרת וכך נמנעות פריצות רבות. ישנם שירותים מתקדמים בתשלום אך לרוב יספיק להשתמש בשירות של חברת CLOUDFLARE, אמנם יש לדעת שאם לא יודעים כיצד להגדיר את השירות עלולות להיות בעיות בגישה לשרת וכן יש לדעת שהמעבר לשימוש ב-CloudFlare דורש שינוי DNS.

לינקים:
1. CloudFlare – חינמי (יש גם תוכניות בתשלום): https://www.cloudflare.com/
2. INCAPSULA – מוצר מעולה אך בתשלום: https://www.imperva.com/products/web-application-firewall-waf/

גיבוי

מכיוון שלעולם לא ניתן לחסום אתר ב-100%, חשוב מאוד שתהיה תכנית גיבוי מסודרת לאתר או לשרת שלכם.
אנו ממליצים על גיבוי נוסף לגיבוי שיש באחסון על מנת להיות בטוחים. פוליסת גיבוי לרוב מנוהלת ע"י מנהל השרת ובמקרה של השרתים השיתופיים אנו מגדירים גיבוי לכשבועיים אחורה.
חשוב שיהיה לכם גיבוי גם לחודש או חודשיים אחורה ושיהיה שמור אצלכם במחשב הפרטי. זאת משום שבמידה והפרצה קיימת ליותר מהשבועיים האחרונים, כלום לא יעזור כי גם כל הגיבויים כבר עם קוד נגוע., למקרה כזה עליכם לשמור כל חודש או חודשיים (ויש ששומרים אף יותר מזה) גיבוי שמהווה רשת בטחון.

לינקים:

1. בשרתי פלסק ניתן לעשות גיבוי ל-FTP, ראו: https://support.plesk.com/hc/en-us/articles/115000148685-How-to-configure-FTP-backup-in-Plesk (בחלק הנקרא: "For individual subscription backup")
2. עבור אתרי WordPress ניתן ומומלץ להשתמש בפלאגין גיבוי בו אפשר להגיר גיבוי אף ל-Google Drive או Dropbox ודומיהם. דוגמה לפלאגין גיבוי: https://wordpress.org/plugins/backwpup/

סיכום

האבטחה של האתר שלכם (ושל השרת שלכם) תלויה בכם. אם תקראו בדקדוק את המאמר ותיישמו את הנאמר בו, הסיכויים שתיפרצו קטנים בצורה דרסטית.
אנו באינטרספייס עשינו כבר את כל האפשר להגן ברמת חומרה על השרת שלכם, לרבות הקשחות, גיבויים, ניהול הרשאות, פיירוול, הזמנת ביצוע ניסיונות פריצה "ידידותיים" ע"י חברות אבטחת מידע ועוד...

שימרו על עצמכם! שלכם, אינטרספייס בע"מ

מותגים מבית טוב