راهنمای حل مشکل امنیتی

موجود بر روی FTP

راهنمای حل مشکل امنیتی موجود بر روی FTP
تاریخ تنظیم: مرداد۱۳۹۸
گروه شرکت‌های شاتل

فهرست مطالب

FTP چیست

FTP یکی از قدیمی‌ترین پروتکل‌های اینترنت است که در سال ۱۹۷۰ در اینترنت توسعه یافت و هنوز هم کاربرد زیادی دارد. FTP مخفف File Transfer Protocol است که یک پروتکل استاندارد در TCP/IP است. مانند HTTP که محتوای وب را منتقل می‌کند یا SMTP که ایمیل‌ها را منتقل می‌کند FTP هم ساده‌ترین راه برای تبادل فایل از یک کامپیوتر به کامپیوتر دیگر است. این پروتکل از پورت ۲۱ استفاده می‌کند.

چالش‌های امنیتی FTP

پروتکل FTP به‌عنوان یک پروتکل ناامن محسوب می‌شود که دلیل آن ارسال ناامن Username و Password به صورت Clear text و بدون رمزنگاری است. اطلاعاتی که از طریق FTP ارسال می‌شوند به غیر از حملات ساده در مقابل شنود، جاسوسی و حملات Brute force نیز آسیب‌پذیر هستند.

چندین روش رایج برای مقابله با این چالش‌ها و امن سازی استفاده FTP وجود دارد. FTPS توسعه ای از FTP است که می‌تواند ارتباط را به درخواست Client رمزنگاری کند. SSL, TLS و SSH راه‌حل‌های امن جایگزین FTP هستند که از ارتباط رمزنگاری‌شده استفاده می‌کنند.

نکات اصلی امن سازی سرورهای FTP و FTPS

لزوم استفاده از FTP را بررسی کنید

بررسی کنید که آیا به‌راستی نیاز است که از FTP در شبکه خود استفاده کنید یا خیر؟ در صورت عدم نیاز به این سرویس حتماً آن را در شبکه خود غیرفعال کنید.

FTP را جایگزین کنید

اگر بروی سرور خود از FTP استفاده می‌کنید، باید در اولین فرصت آن را غیرفعال کنید. از توسعه FTP بیش از ۳۰ سال می گذرد و برای مقاومت در مقابل تهدیدات امنیتی مدرن طراحی نشده است. FTP فاقد حریم خصوصی است و هکرها می‌توانند به‌راحتی به داده‌هایی که در حال انتقال است دسترسی داشته باشند و داده‌ها را دریافت کنند و آنها را تغییرات دهند.

پیشنهاد می‌شود از جایگزین های امن دیگری برای FTP استفاده کنید مانند : FTPS , SFTP

از رمزنگاری قوی و هش کردن (Hashing) استفاده کنید

ارتباط رمزگذاری شده در هر دو پروتکل SFTP و FTPS برای حفاظت از داده‌ها در حین انتقال استفاده می‌شود. رمزنگاری یک الگوریتم پیچیده است که داده‌های اصلی را می‌گیرد و با استفاده از یک کلید، داده‌های رمزگذاری شده را برای انتقال ایجاد می‌کند. اولین کاری که باید انجام دهید این است که هرگونه رمزهای قدیمی مانند Blowfish و DES را غیرفعال کنید و تنها از رمزهای قوی مانند AES یا TDES استفاده کنید.

DMZ Gateway را قبل از شبکه داخلی خود قرار دهید

DMZ بخش مشترکی از شبکه است که برای ذخیره سرورها استفاده می شود اما مشکل DMZ این است که با اینترنت عمومی در ارتباط است و باعث می‌شود تا شبکه شما آسیب‌پذیرتر شود و موردحمله واقع شود. اگر سرور FTP در DMZ باشد، بازهم امنیت در شبکه شما برقرار نخواهد بود.

یک رویکرد مناسب برای ایمن کردن FTP سرور ، استفاده از یک DMZ Gateway یا یک Reverse Proxy است. با استفاده از این روش شما می‌توانید کنترل بیشتری بر ورودی‌های خود داشته باشید.

IP Blacklistsو IP Whitelists را پیاده سازی کنید

برای ایجاد ارتباط با سرورهای خود، سعی کنید لیست مشخصی از IP های مجاز و غیرمجاز تهیه‌کرده و آن را بر روی Firewall های نرم‌افزاری و یا سخت‌افزاری خود محدود کنید.

برای اولین راه، حتماً ارتباط با سرورهای خود را از طریق سرورهای خارج از ایران ببندید.

غیر فعال کردن سرویس FTP در میکروتیک

درصورتی‌که در شبکه داخلی دستگاه میکروتیک دارید و از سرویس FTP استفاده‌ای ندارید خواهشمندیم برای حفظ امنیت شبکه داخلی‌تان از مسیر زیر در کنسول دستگاه میکروتیک اقدام به غیرفعال سازی این سرویس بفرمایید .