مشتریان محترم مرکز داده تبیان

حفظ امنیت و دستیابی به کارایی بهینه، هدف اصلی مرکز داده اینترنتی تبیان می باشد لذا در این راستا کنترل ترافیک شبکه مرکز داده و جلوگیری از حملات احتمالی از وظایف مرکز داده تبیان می‌باشد. از سوی دیگر همانطور که در SLA سرویسهای مرکز داده نیز مشخص شده است، عدم استفاده از سیستم‌ها و نرم افزارهایی که باعث اختلال در عملکرد شبکه شده و زمینه ایجاد حملات از این مرکز داده را فراهم می نمایند نیز، از تعهدات مشتریان محترم می‌باشد. با توجه به اینکه در چند روز اخیر مشاهده شده است که حملات موفق DNS Flood به سرویس های DNS واقع در این مرکز داده انجام می‌گردد، این موضوع بیانگر این است که سرویسهای DNS متعلق به مشتریان محترم بدون امن سازی کافی نصب شده‌اند و به همین دلیل زمینه موفقیت این حملات را فراهم آورده‌اند. لذا لازم است مشتریان محترمی که بر روی سرورهای خود، سرویس DNS راه-اندازی نموده‌اند، جهت پیشگیری از تکرار این حملات، سریعاً نسبت به امن سازی این سرویس اقدام نمایند.

حداقل امن سازی مورد نیاز برای انجام این کار در دو حالت توضیح داده شده است که مشتریان محترم می‌توانند با انجام حالت مناسب اقدام به امن‌سازی سرویس DNS خود نمایند:

1. **بستن دسترسی Recursive Query**

در صورتی که سرویس DNS تنها نقش NS دامنه را به عهده دارد، لازم است که حتما Recursive Query بسته شود، بدین ترتیب DNS به درخواست های دریافتی برای Resolve کردن دامنه های خارج از دامنه‌ی مشتری (مانند yahoo.com، iran.ir ،...) پاسخ نمی‌دهد. در ادامه روش انجام این امن‌سازی در نرم افزارهای bind و MS DNS ذکر شده است:

a. **روش انجام امن سازی در نرم افزار bind:**

پیکربندی موارد زیر در فایل named.conf باید به شکل زیر تنظیم شده باشند:

```
allow-recursion{“none”;};
recursion no;
```

b. روش انجام امن سازی در نرم افزار MS DNS

با اجرای cmd در Run وارد محیط command prompt شوید و دستور زیر را اجرا کنید:

```
C:\>dnscmd %computername% /Config /NoRecursion 1
```

خواهشمند است توجه فرمایید، در صورت بروز اخلال به دلیل عدم امن سازی تذکر داده شده، مرکز داده مجبور به قطع ترافیک مشتری خواهد بود.

با احترام

مرکز داده اینترنتی تبیان