

سلاح‌های پنتاگون «به راحتی» و با «ابزارهای ابتدایی» قابل هک هستند - دیجیاتو

شایان ضیایی | دوشنبه، ۲۳ مهر ۱۳۹۷

دیوان محاسبات آمریکا، آژانسی فارغ از جبهه گیری های سیاسی که به درخواست کنگره این کشور به بررسی مسائل مختلف می پردازد در تازه ترین گزارش خود اعلام کرده که سیستم های تسلیحاتی جدید آمریکا -مانند جت F-35، سیستم های موشکی و دیگر ابزارآلات پیشرفته- برای مقابله با حملات سایبری آمده نیستند و می توان آنها را «به راحتی» و به کمک «ابزارهای ابتدایی» هک کرد.

این آژانس از کشف آسیب پذیری هایی سایبری در تمام سیستم های تسلیحاتی در حال ساخت آمریکا خبر داده و می گوید این آسیب پذیری ها می توانند بسیاری از مأموریت های نظامی را به خطر بیندازند. گفته می شود یکی از مهم ترین آسیب پذیری ها، قابلیت های مبتنی بر نرم افزار در سیستم های موشکی و هواگردها هستند.

درست همانطور که اینترنت به بخش مهمی از زندگی روزانه ما تبدیل شده، نقشی اساسی در سیستم های تسلیحاتی پنتاگون نیز ایفا می کند. به عنوان مثال کلاهخود خلبانان جت F-35 به تنهایی به چند دیتا فید پیچیده از چند سیستم خارجی متصل می شود. همین اتصال به اینترنت باعث ایجاد آسیب پذیری هایی در تسلیحات آمریکا شده و دیوان محاسبات می گوید پنتاگون در برطرف سازی این آسیب ها عملکردی بسیار فاجعه بار داشته است.



به عنوان مثال پنتاگون حتی به خود زحمت نداده که پسورد پیش فرض «چندین» سیستم تسلیحاتی که از نرم افزارهای متن باز یا تجاری استفاده می کنند را تغییر دهد؛ در واقع چگونگی استفاده آنها از تازه ترین فناوری های نظامی جهان، تفاوتی با چگونگی استفاده یک شخص تنبل از روتر خانگی اش ندارد. در بخشی دیگر از گزارش دیوان محاسبات آمده که حتی با تست های خود پنتاگون هم می توان دریافت که هک این سیستم ها تا چه حد آسان است.

این آژانس می گوید که از سهولت هک سیستم های پنتاگون کاملاً تعجب زده شده است. «در یک مورد، تیمی دو نفره تنها ظرف 1 ساعت قادر به دسترسی ابتدایی به یک سیستم تسلیحاتی بودند و بعد از یک روز، کنترل کامل سیستمی که در حال تست بود به دست گرفته شد». در تست های دیگر امکان به دست گرفتن ترمینال یک اپراتور، نمایش پیغام های پاپ آپ برای اپراتورها و همچنین کپی یا حذف کردن اطلاعات نیز وجود داشت؛ حتی یکی از تیم ها موفق به دانلود 100 گیگابایت اطلاعات محرمانه شد.

[دیجیاتو](#)