چهار شنبه 19 مرداد 1390 - 09:35

بدن انسان قرباني بعدي جنايات سايبري

محققان علوم رایانه ای و متخصصان امنیت شبکه معتقدند قربانی بعدی جنگ ها و جنایت های سایبری می تواند بدن انسان ها باشد.

دن انسان قرباني بعدي جنايات سايبري
جام جم آنلاین: محققان علوم رایانه ای و متخصصان امنیت شبکه معتقدند قربانی بعدی جنگ ها و جنایت های سایبری می تواند بدن انسان ها باشد.
به گزارش مهر، «جی ردکلیف» متخصص امنیتی شرکت IBM و محقق دانشگاه «وین استیت» در مقاله ای با عنوان «هک کردن تجهیزات پزشکی برای سرگرمی و انسولین» نشان داده است چگونه هکرها می توانند از راه دور دو ابزار پزشکی که برای درمان دیابت به کار گرفته می شوند را هک کرده و آنها را از کار بیاندازند که نتیجه این کار می تواند فاجعه بار باشد.

«ردکلیف» که خود نیز به دیابت مبتلا است، چهار ماه به مطالعه بر روی ایده امکان هک شدن ابزارهای گلوکز سنج CGM ویژه دیابتی ها پرداخت، حسگر بی سیمی که به بدن انسان وصل شده و هر پنج دقیقه قند خون را بررسی کرده و اطلاعات آن را به ابزار کنترل کننده ای ارسال می کند.

وی همچنین برای چندین ماه بر روی پمپ های انسولینی که می توانند از طریق لوله های زیرپوستی انسولین را به بدن بیمار تزریق کنند کار کرد تا توانست امکان هک کردن آنها را نیز به اثبات برساند.

به گفته «ردکلیف»، ارتباطات بیسیم با پمپ های انسولین به هیچ وجه ایمن نیستند، این ارتباطات قابلیت به روز رسانی نداشته و هیچ راهی برای ترمیم آنها وجود ندارد. این ویژگی درباره CGM ها نیز صدق می کند و این ابزارها نیز در برابر هکرها بسیار آسیب پذیرند.

وی با نفوذ به درون ویژگی های فنی CGM ها دریافت که ارتباط میان حسگرهای بدن و ابزار کنترل کننده این حسگرها یک جهته بوده و این به آن معنی است که حسگرها هیچ اطلاعاتی درباره ابزاری که اطلاعات آنها را دریافت می کنند، ندارند.

متخصص امنیتی شرکت IBM سپس با تجزیه حسگرهای کنترل کننده قند خون دریافت تراشه درون آن مشابه تراشه هایی است که در سامانه های کنترل سرپرستی و گردآوری اطلاعات یا SCADA به کار گرفته می شوند، شبکه خودکار رایانه ای که کنترل سیستمهای صنعتی را به عهده دارد.

وی سپس حملاتی را به دستگاه CGM آغاز کرد که به واسطه این حملات دستگاه ارسال سیگنال به کاربر خود را متوقف کرد.

«رد کلیف» ثابت کرد در صورتی که بتوان خروجی سیگنالهای این دستگاه را مسدود کرده، آن را مختل ساخته و دوباره به حسگرها بازگرداند می توان به این شکل بیمار دیابتی را درباره میزان قند خون بدنش به اشتباه انداخت. به گفته ردکلیف انجام چنین حمله مخربی به پمپ های انسولین ساده تر است.

وی پس از بررسی ویژگی های پمپ انسولین کد مخربی را نوشت و آن را با کمک ابزار USB که می تواند از طریق فرکانس های رادیویی ارتباط برقرار کند در پمپ فعال کرد و توانست با استفاده از آن پمپ را خاموش کند. رویدادی که در صورت عدم اطلاع بیماری می تواند منجر به اختلال بینایی و آسیبهای شدید کلیه شود و در صورت ادامه یافتن این شرایط بیمار آغاز به تعریق کرده و قدرت کنترل بدن خود را از دست خواهد داد و تنفسش دچار مشکل شده و به تدریج خواهد مرد.

متخصص امنیتی شرکت IBM معتقد است تحقیقات وی نشانگر غیر ایمن بودن تمامی ابزارهای مدرن هستند، ابزارهایی که به صورت روزانه مورد استفاده قرار می گیرند و برخی از آنها با بقای انسان ها در ارتباط مستقیم اند.

«رد کلیف» می گوید: خطر همیشه در کمین است، ما نمی توانیم آن را انکار کرده و بگوییم این فقط یک پمپ انسولین است، پس کسی آن را هک نخواهد کرد! این جمله ای است که 15 سال پیش درباره اینترنت گفته می شد. امروز باید دقت بیشتری به چنین مواردی شود، تنها این که هک کردن چنین ابزارهایی کار سختی است نمی تواند به معنی این باشد که ابزارها هک نخواهند شد زیرا امروز در جهان انسانهای باهوش زیادی زندگی می کنند.