Hacker có thể điều khiển từ xa việc bơm insulinm, thay đổi kết quả nồng độ đường trong máu, và người ta đã minh họa thành công vụ tấn công nhằm vào máy trợ tim và máy khử rung tim.
Mọi thứ có thể gây hậu quả nghiêm trọng.

Kết quả trên do nhà nghiên cứu bảo mật Jay Radcliffe phát hiện ra trong thời gian điều trị bệnh tiểu đường. Hành vi này có thể khiến bệnh nhân nhận được quá nhiều hoặc quá ít insulin, một loại hóc môn cần thiết để đảm bảo trao đổi chất diễn ra bình thường.

Jay Radcliffe đã thí nghiệm ngay trên thiết bị của mình. Radcliffe cho biết *"ban đầu tôi cảm thấy vấn đề kĩ thuật này khá thú vị. Tuy nhiên sau đó tôi vô cùng kinh hoàng khi nghĩ tới việc các thiết bị bảo vệ mạng sống của mình không hề được bảo mật."*

Ngày càng có nhiều thiết bị y tế như máy trợ tim, các thiết bị phẫu thuật như điện cực kích thích sâu não có khả năng truyền thông số từ cơ thể bệnh nhân tới máy tính của bác sỹ. Một số các thiết bị có thể điều khiển từ xa bởi chuyên gia y tế. Mặc dù không có bằng chứng cho thấy có người đã từng sử dụng kỹ thuật của Radcliffe, phát hiện của ông gây ra mối lo sợ về sự an toàn của các thiết bị y tế trong thời đại Internet. Người ta đã minh họa thành công một số vụ tấn công nghiêm trọng nhằm vào máy trợ tim và máy khử rung tim.

Các nhà sản xuất thiết bị y tế đánh giá thấp các nguy cơ từ những cuộc tấn công kiểu này. Họ lập luận rằng các cuộc tấn công được minh họa đều do các nhà nghiên cứu bảo mật lành nghề thực hiện và không có khả năng xảy ra ngoài đời thật. Mặc dù các nhà sản xuất đã nỗ lực tự động hóa các thiết bị y tế và gắn thêm các chip không dây, các thiết bị này thường quá nhỏ để gắn thêm vi xử lý đủ mạnh để thực hiện mã hóa tiên tiến nhằm thay đổi tần số, ngăn chặn nghe lén thông tin trao đổi từ thiết bị với máy tính. Lỗ hổng chính là nằm ở đây.

Radcliffe sử dụng bơm tiêm insulin có điều khiển từ xa để điều chỉnh lượng insulin. Ông phát hiện ra rằng bơm tiêm này có thể bị lập trình lại và điều khiển bởi một người lạ mặt. Tất cả những gì ông cần có là một thiết bị kết nối USB bán sẵn trên eBay hoặc các công ty cung cấp thiết bị y tế. Bằng cách nhìn vào dữ liệu được truyền từ máy tính có cắm USB với bơm insulin, ông có thể điều khiển bơm thông qua USB. Radcliffe cho biết các loại bơm insulin do các hãng khác nhau sản xuất đều có khả năng bị tấn công. Mặc dù để tấn công, hacker cần ngồi cách đối tượng khoảng vài mét, một người lại mặt đi lại trong bệnh viện hoặc ngồi sau bệnh nhân trên máy bay cũng ở phạm vi đủ gần để tấn công.

Các quan chức của Cơ quan Quản lý Thuốc và Thực phẩm Hoa Kỳ (FDA) từ chối bình luận cụ thể về kết quả nghiên cứu của Radcliffe. Các quan chức ngành công nghiệp thì coi "nguy cơ thiết bị của một bệnh nhân tiểu đường bị hack là cực kì nhỏ, và đối với thiết bị y tế, nguy cơ thiếu quản lý, giám sát nguy hiểm hơn nguy cơ bị hack rất nhiều"

Radcliffe nói rằng mục đích của cuộc nghiên cứu không phải để cảnh báo mọi người. Điều quan trọng là các vấn đề đó phải được công bố khi ngành công nghiệp y tế ngày càng phát triển nhiều loại thiết bị kết nối mạng.

Theo itGate/ ICTnews/ Huffingtonpost