Một trong những thách thức lớn nhất trong bảo mật ngày nay là làm thế nào để software ở trong hệ thống vận hành và ứng dụng của chúng ta thì **full of holes**. Và trong khi những nhà phát triển phần mêm truyền thống đã làm ra vài hướng đi tiên phong trong việc phát triển nhiều ứng dụng phục hồi, Các chuyên gia cho rằng thiết bị nhúng và nhà phát triển hệ thống từ đó họ tạo ra thiết bị y học được cấy cho hệ thống kiểm soát công nghiệp thì ưu tiên hệ thống bảo mật và phát triển một cách cẩn thận.

Chuyên gia bảo mật phần mềm vá EVP của những sản phẩm và kỹ thuật ở nhà cung cấp dịch vụ bảo mật Perimeter E-Security John Viega nói như thế khi nó trở thành bảo mật hệ thống công nghiệp và nhúng, ông ấy thấy được hai thành quả ở phía trước.

“Nhóm tấn công có thể bắt đầu đòn bẩy để vạch ra cho chúng ta thấy phần dễ bị xâm nhấp trong hệ thống SCADA và làm gì đó thật sự tồi tệ. Điều đó sẽ gây ra sự chú ý, quy tắt và sự đầu tư vào vấn đề này” Viega nói.

Đó là một kết quả. Các kết quả khác thì là những điểm yếu khó chịu lặng lẽ trong một thời gian dài và không thể hoàn thành.” Nếu đó không phải là sự tình cờ, vấn đề này sẽ không tự sửa mọt cách nhanh chóng. Nhiều người sẽ trở nên bão hóa cho đến khi thứ gì đó tồi tệ sẽ xảy ra. Họ sẽ gọi đó là mố đe dọa lý thuyết. Tuy nhiên, chúng ta biết rằng tràn bộ đệm lau dài, rất lấu trước khi con người nhận ra sự tồi tệ mà rủi ro đó có thể trở thành” Ông ấy nói.

Nate Kube, trưởng giám đốc kỹ thuật và nhà sáng lập ở