Công Thương
CƠ QUAN NGÔN LUẬN CỦA BỘ CÔNG THƯƠNG
Diễn đàn của giới công thương Việt Nam

Việt Nam thiệt hại tới 542,8 triệu USD do tấn công mạng

00:30 | 09/04/2018 Bản in

Đây là con số báo động do Phó giáo sư Mathews Nkhoma - Trưởng khoa Kinh doanh và Quản trị- Đại học RMIT Việt Nam- đưa ra tại hội thảo "An ninh mạng: Ai làm chủ?" do RMIT Việt Nam vừa tổ chức mới đây.

Theo Phó giáo sư Mathews Nkhoma, việc kết nối mạng phát triển cực nhanh cũng như nhịp độ chuyển đổi kỹ thuật số diễn ra chóng mặt khiến châu Á, đặc biệt là Việt Nam, dễ bị tấn công mạng.

"Theo báo cáo về nguy cơ mạng ở khu vực châu Á Thái Bình Dương do công ty Marsh & McLennan thực hiện năm 2017, các tổ chức và doanh nghiệp ở châu Á mất 1,7 lần lâu hơn các nơi

khác trên thế giới để phát hiện ra một vụ tấn công, và 78% người dùng Internet ở châu Á không được đào tạo gì về an ninh mạng"- ông Mathews Nkhoma cho biết.

Ông nhấn mạnh rằng, Việt Nam nằm trong nhóm 10 quốc gia dễ bị nhắm đến nhất và là mục tiêu của tấn công mạng từ năm 2015 đến 2017. Riêng năm 2017, Việt Nam đã mất 542,8 triệu USD do tấn công mạng.

Cũng tại đây, Giáo sư Matthew Warren - Phó giám đốc Trung tâm nghiên cứu An ninh mạng của Đại học Deakin - nhận định: an ninh mạng là yếu tố nền tảng của sự phát triển và thịnh vượng của một quốc gia trong kinh tế toàn cầu, và quan trọng với an ninh quốc gia. "Nguy cơ và lỗ hổng an ninh toàn cầu hiện ảnh hưởng tới mọi tổ chức và khách hàng của họ. Tính chất phức tạp của an ninh mạng khiến các tổ chức càng khó hiểu các nguy cơ và vì vậy khó kiểm soát an ninh mạng"- Giáo sư Warren cho biết.

Ông còn nhấn mạnh đến mối liên kết giữa nguồn lực con người và sự phức tạp trong duy trì an ninh. Nhìn từ quan điểm an ninh mạng, nguồn tài nguyên con người có thể thất bại do thiếu kinh nghiệm, đào tạo không phù hợp và giả định sai. Vì vậy, đầu tư vào phát triển kỹ năng mạng, cũng như tuyển dụng và duy trì đội ngũ nhân viên an ninh mạng là việc hết sức quan trọng cho các tổ chức.

"Hiện còn thiếu một triệu chuyên gia an ninh mạng trên toàn cầu", Giáo sư nói và bổ sung thêm rằng con số này dự báo sẽ tăng lên 1.5 triệu vào năm 2019. Về những kỹ năng cần có ở chuyên gia an ninh mạng tương lai, Giáo sư Warren cho biết họ sẽ cần chuyên môn kỹ thuật để vận hành những kỹ thuật an ninh trọng yếu, kỹ năng tổ chức để định hướng chính sách và nguy cơ, kỹ năng liên quan con người để làm việc với người khác, và kỹ năng mềm để giao tiếp.

Cùng chung quan điểm về yếu tố "con người", Phó giáo sư Nkhoma kêu gọi các tổ chức nên chuyển đổi từ phân tích kinh doanh sang phân tích con người.

Trong một tổ chức, những người thường đưa ra lời khuyên liên quan đến an ninh và công nghệ là những người có ảnh hưởng lớn nhất lên hành vi an ninh thông tin. "Một khi nhận diện được những người này, chúng ta có thể xây dựng chiến lược và làm việc cùng với họ, đồng thời nâng cao an ninh của cả tổ chức"- Phó giáo sư Nkhoma chia sẻ.

Nguyễn Phượng