lao động phàn nàn về công tác hỗ trợ triển khai, đồng thời giao chỉ tiêu phấn đấu cụ thể cho các đơn vị và các cán bộ chuyên trách. Kế hoạch tổ chức các buổi tập huấn cũng như hỗ trợ cài đặt, kết nối giúp doanh nghiệp thực hiện giao dịch điện tử phải được bảo đảm thực hiện đúng tiến độ yêu cầu. Những khó khăn vướng mắc được giải quyết nhanh chóng, triệt để với sự cơ động của Tổ hỗ trợ. Đến thời điểm hiện tại, hầu hết các doanh nghiệp đã được hỗ trợ với tinh thần trách nhiệm cao nhất từ phía cơ quan BHXH. BHXH tỉnh cũng đã yêu cầu cơ quan cung cấp dịch vụ đường truyền internet bảo đảm, nâng cấp tốc độ đường truyền, tránh để ảnh hưởng đến quá trình giao dịch của doanh nghiệp. Đường dây nóng của BHXH tỉnh thiết lập hỗ trợ doanh nghiệp cũng đã và đang hoạt động hết sức tích cực.

Các nội dung công việc khác cũng đã được triển khai với tinh thần khẩn trương, nhanh chóng. Đến thời điểm hiện tại, BHXH tỉnh đã hoàn thiện xong cơ sở dữ liệu quá trình tham gia BHXH, BHYT của cá nhân, tổ chức để kết nối trong toàn tỉnh; sẵn sàng tập trung gửi về dữ liệu chung của Ngành BHXH. Đáng nói hơn, tính đến hết ngày 31/8/2015, đã có 1.142/1.229 đơn vị được tập huấn và thực hiện thành công giao dịch điện tử, tương đương 93%. Có thể nói, đây là kết quả rất đáng ghi nhận với một tỉnh miền núi như Bắc Kạn; những khó khăn ban đầu đã được cơ bản giải quyết. Đây sẽ là cơ sở quan trọng để BHXH tỉnh Bắc Kạn làm tốt hơn nữa công tác tổ chức thực hiện BHXH, BHYT cho người dân trên địa bàn. Các doanh nghiệp sẽ được tạo điều kiện thuận lợi hơn trong quá trình thực hiện các thủ tục BHXH, BHYT, những khó khăn mang tính đặc thù của giao thông miền núi sẽ không còn là trở ngại quá lớn.■

TĂNG CƯỜNG CÔNG TÁC BẢO MẬT - AN TOÀN HỆ THỐNG THÔNG TIN

✍ NGUYỄN THỊ LAN HƯƠNG
BHXH TỈNH BÌNH ĐỊNH

Công nghệ thông tin không chỉ có ứng dụng quan trọng trong công việc hàng ngày mà còn góp phần to lớn trong cải cách thủ tục hành chính, đổi mới lề lối làm việc và công tác quản lý nhà nước từ Trung ương đến địa phương, trên cơ sở áp dụng hệ thống thông tin điều hành tác nghiệp. Đồng thời, cung cấp kịp thời, đầy đủ, chính xác, nhanh chóng các thông tin, tài liệu điện tử, giảm đáng kể các thủ tục phiền hà cho đối tượng trong các quan hệ giao dịch, tiết kiệm các chi phí giấy mực in ấn...

Hiện nay, các cá nhân, doanh nghiệp có thể làm thủ tục hải quan, kê khai thuế và nộp thuế; gửi hồ sơ tham gia, đóng và hưởng BHXH, BHYT và thực hiện các dịch vụ công điện tử trong lĩnh vực tài chính qua mạng internet. Các cấp, ngành có thể tiết kiệm thời gian và giảm bớt chi phí đi lại, ăn, ở cho các cuộc họp tập trung bằng cách họp trực tuyến. Các bệnh viện về tỉnh đã sử dụng hệ thống chẩn đoán, chữa bệnh từ xa, bất cứ khi nào gặp ca bệnh khó, phức tạp vượt quá khả năng chuyên môn, các bác sĩ tuyến cơ sở đều có thể yêu cầu tư vấn, hỗ trợ từ xa để được hướng dẫn chẩn đoán, điều trị bệnh chính xác cho bệnh nhân... Tuy nhiên, ngoài những giá trị to lớn, hệ thống CNTT và mạng internet cũng đem đến không ít hiểm họa khôn lường, gây ra những tổn thất nghiêm trọng cho cá nhân, doanh nghiệp, cơ quan nhà nước khi những thông tin quan trọng bị rò rỉ ra ngoài. Đó có thể là dữ liệu tài sản thuộc sở hữu trí tuệ, thông tin về khách hàng, các cơ sở dữ liệu quan trọng của hệ thống, thậm chí cả những thông tin giao dịch tài chính của ngân hàng, các

thông tin bảo mật của cơ quan nhà nước bị hacker đánh cắp lợi dụng. Và nguy cơ xảy ra chiến tranh mạng và tội phạm mạng đang đe dọa đến các chính phủ, các tổ chức xã hội, cơ quan, doanh nghiệp và người dân. Trong đó, giới trẻ là những người dễ bị tác động và ảnh hưởng nhất. vì giới trẻ vừa "nhạy cảm" với đổi mới về công nghệ, vừa chưa có đủ năng lực để nhận thức đúng đắn về tác động mặt trái của các vấn đề an ninh mạng, cũng như chưa thể tự bảo vệ mình trước các loại hình tội phạm mạng, chiến tranh mạng ngày càng diễn ra tinh vi, thường xuyên hơn.

Những năm qua, cảnh sát phòng chống tội phạm sử dụng công nghệ cao, cục an ninh tài chính tiền tệ, cục an ninh truyền thông đã phát hiện và xử lý nhiều vụ án phức tạp do tội phạm công nghệ cao gây ra. Chúng đã thực hiện hành vi chiếm đoạt tài sản bằng cách đánh cắp mật khẩu tài khoản ngân hàng, cài đặt phần mềm trái phép vào máy chủ của ngân hàng để thực hiện lệnh chuyển tiền, mua bán thông tin cá nhân... để thu lợi bất chính hàng tỷ đồng. Ngoài ra, còn tấn công làm thay đổi giao diện; từ chối dịch vụ nhiều website quan trọng; giả danh nhà mạng, nhắn tin, gọi điện báo trúng thưởng để lừa tiền của những người dân thiếu hiểu biết; lập những trang web cá độ bóng đá trực tuyến để lôi kéo dụ dỗ, cho vay nặng lãi và làm cho không ít người khuynh gia bại sản hoặc rơi vào vòng lao lý... Hầu hết các cuộc tấn công tập trung lừa đảo người dùng điện thoại, mạng internet đều vì mục tiêu tài chính. Vì vậy, cần cài đặt các phần mềm diệt virus có bản quyền uy tín, hiệu quả để phát hiện, ngăn chặn việc máy tính bị xâm phạm trái phép. Không truy cập vào các đường link, cảnh báo, các phần mềm như trúng thưởng, diệt virus xuất hiện trên các trang web. Nếu phát hiện tiền trong tài khoản bị mất cắp thì người bị hại cần nhanh chóng thông báo ngay cho ngân hàng và cơ quan công an để có biện pháp xử lý, tiến hành điều tra.

Theo thông báo số 105/TB-BCA-A61 ngày 07/10/2013 của Bộ Công an về nguy cơ mất an ninh mạng khi sử dụng hệ điều hành Windows XP sau thời điểm Microsoft kết thúc các dịch vụ và hỗ trợ hệ điều hành này, Thông báo số 106/TB-BCA-A61 ngày 07/10/2013 của Bộ Công an về nguy cơ mất an ninh thông tin qua thiết bị di động thông minh; đồng thời, ngày 31/10/2014, phiên bản hệ điều hành Windows 07 bị Microsoft ngừng hỗ trợ. Như vậy, những máy đã cài đặt các phiên bản bao gồm Windows 07 Home Basic, Home Premium hoặc Ultimate... sẽ không còn nhận được bản vá lỗi cập nhật nữa, ngoại trừ Windows 07 Professional cho doanh nghiệp. Tuy nhiên, hiện nay phần lớn máy tính đang sử dụng ở các cơ quan vẫn còn dùng windowsXP và Windows 07, vì vậy, để chống lại các loại hình tấn công có chủ đích, người sử dụng máy tính cần được đào tạo về kỹ năng bảo mật an toàn hệ thống thông tin; tránh mở những tập tin, email đáng ngờ, không truy cập vào các đường liên kết không rõ nguồn gốc trong các mạng xã hội; nên thận trọng khi chia sẻ thông tin cá nhân, thông tin liên quan đến cơ quan, đơn vị trên các mạng xã hội... Khi cung cấp số liệu thông tin cho các cơ quan truyền thông như báo, đài phải qua kiểm duyệt của lãnh đạo cấp trên. Đặc biệt, cần chú trọng xóa dữ liệu triệt để trên các ổ cứng máy chủ, máy tính cá nhân khi đưa vào thanh lý tài sản hàng năm.

Các cơ quan, đơn vị cần thông báo rộng rãi đến từng cán bộ, nhân viên về nguy cơ lây nhiễm phần mềm độc hại; tuyên truyền nâng cao nhận thức chấp hành về an toàn an ninh, bảo mật thông tin trong việc sử dụng máy tính truy cập mạng thông tin diện rộng, mạng internet; sử dụng các thiết bị lưu trữ, các thiết bị kết nối ngoài; sử dụng ứng dụng gửi nhận thư điện tử, tải và cài đặt các phần mềm được chia sẻ trên mạng... Người dùng máy tính nên sử dụng các phần mềm bảo mật cho máy tính và cài password bảo vệ những file tài liệu mật. Tuy nhiên, cách này cũng không an toàn đối với những hacker chuyên nghiệp. Hiện nay, sử dụng thẻ thông minh, dấu vân tay, tròng mắt được coi là một phương thức bảo mật hữu hiệu trong việc chứng thực quyền đăng nhập hệ thống. Trong khi chưa được trang bị các kỹ năng và phương tiện bảo mật hệ thống thì người dùng thiết bị tuyệt đối không được kết nối vào mạng internet khi thực hiện việc soạn thảo, biên tập, lưu trữ, xử lý tài liệu, thông tin, dữ liệu mật của cơ quan, đơn vị. Để phòng ngừa bị tấn công, Kaspersky khuyến cáo người dùng một số lưu ý: Không mở những tập tin đính kèm và đường dẫn từ những người không quen biết; thường xuyên chạy phần mềm quét virus máy tính; cẩn thận những tập tin nén chứa file SFX bên trong; cài phiên bản hệ điều hành mới nhất để đảm bảo không bị lỗi; cập nhật các phần mềm từ bên thứ ba như Microsoft Office, Java, Adobe Flash Player và Adobe Reader.

Ông Ngô Tuấn Anh, Phó Chủ tịch phụ trách an ninh mạng của Bkav, cho biết: "Tình hình an ninh mạng trên toàn cầu đang diễn biến ngày càng phức tạp với tần suất các cuộc tấn công nghiêm trọng diễn ra thường xuyên hơn. Tại Việt Nam, chỉ tính từ đầu năm 2015 đến nay, đã có 2.460 website của các cơ quan, doanh nghiệp bị xâm nhập". Trong khi đó lực lượng chuyên gia an ninh mạng trong nước lại quá mỏng và yếu. Vì vậy, cần có các chương trình đào tạo thường xuyên cho đội ngũ cán bộ làm công tác an ninh mạng, quản trị mạng ở cơ quan nhà nước, doanh nghiệp để góp phần tăng cường nhân lực an ninh mạng và kịp thời ứng phó với mọi hiểm họa từ mạng internet. Các cơ quan,

đơn vị cần thành lập bộ phận chuyên trách về vấn đề tăng cường bảo mật và đảm bảo an toàn hệ thống an ninh mạng, thường xuyên thực hiện kiểm tra toàn bộ hệ thống máy tính của cơ quan nhằm phát hiện các lỗ hổng bảo mật hệ thống, lây nhiễm các phần mềm độc hại; cô lập và khắc phục kịp thời, tiêu diệt triệt để bảo đảm không để các phần mềm độc hại có điều kiện lây nhiễm, phát tán; thường xuyên cập nhật các bản vá lỗi mới nhất cho hệ điều hành và các ứng dụng để phòng khả năng lây nhiễm, hoạt động của các phần mềm độc hại. Đồng thời, đưa ra giải pháp, cơ chế bảo mật cho hệ thống mạng. Thường xuyên cung cấp các lưu ý, cảnh báo liên quan đến an toàn bảo mật thông tin nhằm tránh các rủi ro đáng tiếc xảy ra.

Cần tăng cường củng cố đội ngũ cán bộ văn thư, lưu trữ có phẩm chất năng lực, trình độ chuyên môn, chuyên nghiệp và cơ sở vật chất nhằm đảm bảo an toàn và bảo mật tài liệu hiện hành cũng như tài liệu lưu trữ.

Tóm lại, mọi hoạt động của xã hội hiện nay đều gắn với các ứng dụng công nghệ thông tin, từ giao dịch, giải trí... đến các hoạt động xã hội, kinh tế, văn hóa, giáo dục, y tế...; thuật ngữ thương mại điện tử, chính phủ điện tử, văn phòng không giấy mực... không còn xa lạ nữa, do đó vấn đề an ninh mạng trở thành một trong những vấn đề được chú trọng, quan tâm hàng đầu. Vì vậy, mỗi người cần không ngừng nâng cao hiểu biết về công nghệ, cách bảo mật an toàn hệ thống thông tin để bảo vệ bản thân, cơ quan, doanh nghiệp, tránh kẻ xấu lợi dụng gây ra tổn thất đáng tiếc. Bên cạnh đó, đem những kiến thức, kỹ thuật, công nghệ tiên tiến, hiện đại phục vụ nhân dân nhằm đảm tính dân chủ, công khai, minh bạch; tăng cường kiểm tra, giám sát lẫn nhau giữa công dân với cơ quan đơn vị trong môi trường toàn cầu hóa và hội nhập quốc tế.■

Từ khi được chính thức thành lập năm 1975, Cộng hòa Dân chủ Nhân dân Lào luôn chăm lo An sinh xã hội cho tất cả lao động khu vực công, bao gồm công chức, viên chức, lao động làm việc trong doanh nghiệp Nhà nước và các nhân viên làm việc thường xuyên cho Nhà nước. Các chế độ chăm sóc y tế, ốm đau, thai sản, tử tuất và hưu trí được chi trả cho người lao động trên cơ sở không đóng góp và coi là chế độ được hưởng của lao động khu vực công.

ĐỔI MỚI HỆ THỐNG AN SINH XÃ HỘI ở CHDC Nhân dân Lào

✍ MAI OANH
BAN HỢP TÁC QUỐC TẾ, BHXH VIỆT NAM

Do việc chi trả cho chế độ An sinh xã hội ngày càng trở thành gánh nặng cho ngân sách quốc gia, từ năm 1992, Lào bắt đầu thu tiền đóng góp của công chức, viên chức. Theo đó, công chức, viên chức bắt buộc đóng 6% lương cơ bản cho các chế độ An sinh xã hội, Nhà nước sẽ trợ cấp phần chi trả còn lại. Năm 1993, nền An sinh xã hội của Lào chính thức thành lập theo Nghị định số 178/PM của Thủ tướng Chính phủ. Bộ Lao động và Phúc lợi xã hội sẽ thực hiện chính sách An sinh xã hội bao gồm chăm sóc y tế, chế độ ngắn hạn - dài hạn cho công chức, viên chức, quân đội và công an. Trong khi đó, lao động khu vực tư nhân vẫn đứng ngoài diện bao phủ của chính sách An sinh xã hội. Cuối năm 1999, Thủ tướng Chính phủ thông qua Nghị định số 207/PM, chế độ An sinh xã hội mới cho người lao động khu vực tư nhân bắt đầu được thực hiện vào năm 2001 và cơ quan được giao trách nhiệm tổ chức thực hiện là Cơ quan An sinh xã hội Lào (SSO). Năm 2006, Nghị định 70/PM sửa đổi Nghị định 178/PM của Thủ tướng Chính phủ được ban hành, Cơ quan An sinh xã hội khu vực Nhà nước (SASS) được thành lập với nhiệm vụ thực hiện chương trình An sinh xã hội cho lao động khu vực công từ năm 2008. Cả hai cơ quan này đều thực thuộc Bộ Lao động và Phúc lợi xã hội.

Nhận thấy sự chồng chéo giữa cơ quan thực hiện, quy