THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 14 /CT-TTg	*Hà Nội, ngày 07 tháng 6 năm 2019*

CHỈ THỊ
Về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam

Thời gian vừa qua, hành lang pháp lý về an toàn, an ninh mạng của Việt Nam từng bước được hoàn thiện. Tuy nhiên, việc hướng dẫn thi hành pháp luật về an toàn, an ninh mạng, bảo vệ thông tin cá nhân, bảo vệ trẻ em trên môi trường mạng và chế tài xử lý vi phạm còn chưa đầy đủ. Việc xây dựng, ban hành các tiêu chuẩn, quy chuẩn kỹ thuật trong lĩnh vực an toàn thông tin mạng chưa đáp ứng nhu cầu thực tiễn. Hoạt động nâng cao năng lực, nhận thức và trách nhiệm về an toàn, an ninh mạng còn hạn chế. Hợp tác giữa các cơ quan, tổ chức, doanh nghiệp trong và ngoài nước về bảo đảm an toàn, an ninh mạng còn yếu; hoạt động giám sát, đánh giá, bảo vệ hệ thống thông tin trong các cơ quan, tổ chức nhà nước còn thiếu chuyên nghiệp. Trong năm 2018 và đầu năm 2019 đã xảy ra một số cuộc tấn công mạng có chủ đích, đánh cắp thông tin bí mật nhà nước, gây hậu quả nghiêm trọng. Chính vì vậy, xếp hạng của Việt Nam trong Báo cáo chỉ số an toàn, an ninh thông tin toàn cầu (Global Cybersecurity Index - sau đây gọi tắt là GCI) của Liên minh Viễn thông Quốc tế (International Telecommunication Union - sau đây gọi tắt là ITU) còn chưa cao. Theo xếp hạng chưa chính thức tháng 3 năm 2019 (cho giai đoạn 2017 - 2018), Việt Nam xếp thứ 50/194 quốc gia, vùng lãnh thổ được đánh giá, đứng thứ 5/11 trong khu vực Đông Nam Á.

Trong thời gian tới, các cơ quan, tổ chức, doanh nghiệp nhà nước cần triển khai các giải pháp bảo đảm an toàn, an ninh mạng tổng thể nhằm khắc phục các tồn tại, hạn chế nêu trên, góp phần cải thiện hơn nữa xếp hạng của Việt Nam trong GCI. Trên cơ sở đó, Thủ tướng Chính phủ chỉ thị:

1. Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, Tập đoàn, Tổng công ty nhà nước, Ngân hàng thương mại Nhà nước, Ngân hàng Phát triển Việt Nam, Ngân hàng Chính sách xã hội, Ngân hàng Hợp tác xã Việt Nam và các tổ chức tín dụng, tài chính Nhà nước khác thực hiện một số giải pháp sau:

a) Quán triệt nguyên tắc Bộ trưởng, Thủ trưởng cơ quan ngang bộ, cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, Chủ tịch, Tổng giám đốc Tập đoàn, Tổng công ty nhà nước, Ngân hàng thương mại Nhà nước, Ngân hàng Phát triển Việt Nam, Ngân hàng Chính sách xã hội, Ngân hàng Hợp tác xã Việt Nam và các tổ

LuatVietnam
Tiện ích văn bản luật

chức tín dụng, tài chính Nhà nước khác chịu trách nhiệm trước Thủ tướng Chính phủ nếu để xảy ra mất an toàn, an ninh mạng, lộ lọt bí mật nhà nước tại cơ quan, đơn vị mình quản lý;

b) Chỉ định, kiện toàn đầu mối đơn vị chuyên trách về an toàn thông tin mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng. Phối hợp chặt chẽ với cơ quan chuyên trách về an toàn, an ninh mạng của Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng trong giám sát, chia sẻ thông tin, kiểm tra, đánh giá an toàn, an ninh mạng;

c) Đối với công tác giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý: Tự thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực để thực hiện; thông báo thông tin đầu mối thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng về Bộ Thông tin và Truyền thông để tổng hợp trước ngày 31 tháng 12 năm 2019 và khi có sự thay đổi về thông tin đầu mối; kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông;

d) Đối với công tác kiểm tra, đánh giá an toàn thông tin mạng cho hệ thống thông tin thuộc quyền quản lý: Lựa chọn tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật;

Đối với các hệ thống thông tin cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông trước ngày 14 tháng 12 để tổng hợp, báo cáo Thủ tướng Chính phủ;

Đối với hệ thống thông tin quan trọng quốc gia (cấp độ 5), định kỳ 06 tháng một lần thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông trước ngày 14 tháng 6 và ngày 14 tháng 12 hàng năm để tổng hợp, báo cáo Thủ tướng Chính phủ;

đ) Ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ của doanh nghiệp trong nước đáp ứng yêu cầu về an toàn, an ninh mạng theo quy định của pháp luật đối với các hệ thống thông tin cấp độ 3 trở lên, các hệ thống thông tin phục vụ Chính phủ điện tử;

e) Bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin (trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ);

LuatVietnam
Tiện ích văn bản luật

g) Sử dụng và quản lý khóa bí mật (USB token) của chữ ký số, dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ, chứng thư số, các giải pháp mã hóa của Ban Cơ yếu Chính phủ theo đúng quy định;

h) Tiếp tục hoàn thiện cơ chế chính sách, hành lang pháp lý về an toàn thông tin mạng, an ninh mạng, tội phạm mạng, bảo vệ trẻ em trên môi trường mạng; chiến lược, quy hoạch, kế hoạch phát triển an toàn thông tin mạng; phát triển nguồn nhân lực an toàn, an ninh mạng; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng;

i) Kịp thời cung cấp thông tin, số liệu về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác trong lĩnh vực an toàn, an ninh mạng phục vụ việc đánh giá, xếp hạng chỉ số GCI của ITU.

2. Bộ Thông tin và Truyền thông có trách nhiệm:

a) Chủ trì, phối hợp với các bộ, ngành, địa phương liên quan triển khai giải pháp bảo đảm an toàn thông tin mạng tổng thể trong cơ quan, tổ chức nhà nước, các biện pháp nâng cao thứ hạng của Việt Nam về an toàn, an ninh mạng trên thế giới; xây dựng bộ tiêu chí đánh giá mức độ an toàn thông tin mạng của Việt Nam, tổ chức đánh giá và công bố định kỳ hàng năm;

b) Cải thiện hành lang pháp lý, cơ chế, chính sách thúc đẩy an toàn thông tin mạng; trình Thủ tướng Chính phủ phê duyệt chiến lược, quy hoạch, kế hoạch về an toàn thông tin mạng quốc gia các giai đoạn tiếp theo;

c) Chủ trì xây dựng, trình Thủ tướng Chính phủ phê duyệt Đề án đào tạo, phát triển nguồn nhân lực an toàn, an ninh mạng và Đề án tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm bảo đảm an toàn thông tin giai đoạn 2021 - 2025; Đề án về bảo vệ thông tin cá nhân, hỗ trợ trẻ em tương tác lành mạnh, sáng tạo trên không gian mạng;

d) Nghiên cứu, đề xuất sửa đổi quy chế phối hợp giữa Bộ Thông tin và Truyền thông, Bộ Công an và Bộ Quốc phòng trong hoạt động bảo đảm an toàn, an ninh mạng phù hợp với tình hình thực tiễn;

đ) Nghiên cứu, ban hành tiêu chuẩn, quy chuẩn, giải pháp kỹ thuật bảo vệ thông tin cá nhân trong các hệ thống thông tin có thu thập thông tin người dùng trên mạng;

e) Tăng cường công tác tuyên truyền, nâng cao nhận thức và trách nhiệm về bảo vệ trẻ em trên môi trường mạng; chỉ đạo doanh nghiệp cung cấp dịch vụ viễn thông, Internet (ISP), nội dung thông tin số triển khai các giải pháp kỹ thuật về bảo vệ trẻ em trên môi trường mạng;

g) Chủ trì thiết lập, điều hành, tổ chức đào tạo, tập huấn ngắn hạn và dài hạn nhằm nâng cao kiến thức, kỹ năng cho Mạng lưới đơn vị chuyên trách về an toàn thông tin mạng; xây dựng, ban hành tiêu chuẩn kỹ năng cơ bản về an toàn thông tin mạng cho người làm công tác về an toàn thông tin, an ninh mạng trong các cơ quan, tổ chức;

LuatVietnam
Tiện ích văn bản luật

h) Công bố Danh mục sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng đáp ứng được yêu cầu sử dụng trong các cơ quan, tổ chức nhà nước trước ngày 30 tháng 9 năm 2019; định kỳ sửa đổi, bổ sung cho phù hợp với tình hình thực tế;

i) Hướng dẫn, hỗ trợ các cơ quan, tổ chức nhà nước, đặc biệt là cơ quan, tổ chức chưa sẵn sàng về nguồn lực và chuyên môn trong việc giám sát, bảo vệ, kiểm tra, đánh giá an toàn thông tin mạng. Lựa chọn một số cơ quan, tổ chức triển khai thí điểm, trên cơ sở đó, tổ chức sơ kết, đánh giá, nhân rộng mô hình triển khai giải pháp bảo đảm an toàn thông tin mạng tổng thể trong cơ quan, tổ chức nhà nước trước ngày 31 tháng 12 năm 2019;

k) Xây dựng, duy trì vận hành Cổng thông tin điện tử bằng tiếng Việt và tiếng Anh tổng hợp thông tin cần thiết cung cấp cho ITU và các tổ chức uy tín để phục vụ đánh giá chỉ số an toàn, an ninh mạng, bao gồm: văn bản quy phạm pháp luật và chỉ đạo điều hành, báo cáo, thống kê, danh sách doanh nghiệp được cấp phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, các chương trình đào tạo, bồi dưỡng, diễn tập, tài liệu, ấn phẩm tuyên truyền, hoạt động hợp tác trong nước và quốc tế...;

l) Chủ trì đôn đốc, theo dõi thực hiện Chỉ thị này và tổng hợp, báo cáo Thủ tướng Chính phủ kết quả thực hiện hàng năm.

3. Bộ Công an có trách nhiệm:

a) Chủ trì, phối hợp với các cơ quan liên quan tiếp tục hoàn thiện các văn bản quy phạm pháp luật về an ninh mạng, tội phạm mạng và bảo vệ dữ liệu cá nhân;

b) Tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin thuộc lĩnh vực do Bộ Công an chịu trách nhiệm quản lý;

c) Phối hợp chặt chẽ với Bộ Thông tin và Truyền thông trong hoạt động thẩm định cấp độ và bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng quốc gia.

4. Bộ Quốc phòng có trách nhiệm:

a) Tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin thuộc lĩnh vực do Bộ Quốc phòng chịu trách nhiệm quản lý;

b) Phối hợp chặt chẽ với Bộ Thông tin và Truyền thông trong hoạt động thẩm định cấp độ và bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng quốc gia;

c) Ban Cơ yếu Chính phủ có trách nhiệm:

- Chủ trì, phối hợp với các bộ, ngành, địa phương triển khai đồng bộ các giải pháp bảo mật thông tin bí mật nhà nước bằng mật mã kết hợp với việc triển khai, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ, đáp ứng tốt yêu cầu bảo mật, an toàn thông tin tổng thể của các cơ quan Đảng và Nhà nước;

LuatVietnam
Tiện ích văn bản luật

- Tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin thuộc lĩnh vực do Ban Cơ yếu Chính phủ chịu trách nhiệm quản lý.

5. Bộ Kế hoạch và Đầu tư, Bộ Tài chính có trách nhiệm:

a) Tăng cường, ưu tiên bố trí vốn đầu tư phát triển, vốn chi sự nghiệp thường xuyên hàng năm cho các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, các tỉnh, thành phố trực thuộc trung ương triển khai hoạt động bảo đảm an toàn, an ninh mạng;

b) Trong quá trình thẩm định, cân đối nguồn vốn cho các dự án công nghệ thông tin, bảo đảm đạt tối thiểu 10% tổng kinh phí triển khai dự án công nghệ thông tin trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

6. Bộ Giáo dục và Đào tạo có trách nhiệm:

a) Định hướng, hướng dẫn các cơ sở đào tạo ban hành kế hoạch đào tạo nhân lực an toàn, an ninh mạng đáp ứng nhu cầu thị trường;

b) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông đẩy mạnh triển khai các chương trình tuyên truyền, phổ biến, nâng cao nhận thức về an toàn, an ninh mạng trong các cơ sở đào tạo.

7. Bộ Khoa học và Công nghệ có trách nhiệm:

a) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng và các bộ, ngành liên quan hoàn thiện, công bố các tiêu chuẩn, quy chuẩn kỹ thuật trong lĩnh vực an toàn thông tin mạng;

b) Chủ trì, phối hợp với các bộ, ngành liên quan xây dựng cơ chế, chính sách thúc đẩy nghiên cứu - phát triển, khởi nghiệp sáng tạo trong lĩnh vực an toàn, an ninh mạng;

c) Khuyến khích, đẩy mạnh, tăng cường các nhiệm vụ, đề tài nghiên cứu khoa học cấp Bộ và cấp Nhà nước liên quan đến lĩnh vực an toàn, an ninh mạng.

8. Bộ Lao động - Thương binh và Xã hội có trách nhiệm:

a) Chủ trì cải thiện hành lang pháp lý về bảo vệ trẻ em trên môi trường mạng;

b) Tăng cường công tác tuyên truyền, thực thi, cơ chế tương tác, công cụ, phương tiện để bảo vệ trẻ em trên môi trường mạng.

LuatVietnam
Tiện ích văn bản luật

9. Bộ Ngoại giao có trách nhiệm:

a) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, Bộ Công an và Bộ Quốc phòng tăng cường hợp tác, tham gia các tổ chức, thỏa thuận quốc tế song phương, đa phương trong lĩnh vực an toàn, an ninh mạng;

b) Kịp thời chia sẻ thông tin, phản ánh của các cơ quan, tổ chức quốc tế về yêu cầu và đánh giá, xếp hạng an toàn, an ninh mạng cho các bộ, ngành liên quan.

10. Các bộ, ngành, cơ quan và các tổ chức có liên quan có trách nhiệm:

a) Chủ động đăng tải thông tin, số liệu về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác an toàn, an ninh mạng trong lĩnh vực phụ trách lên Cổng thông tin điện tử và các phương tiện truyền thông để hỗ trợ các tổ chức tra cứu, điều tra, khảo sát, thống kê và xếp hạng; bố trí kinh phí cho công tác bảo đảm an toàn thông tin mạng theo điểm e khoản 1 của Chỉ thị này;

b) Phối hợp với Bộ Thông tin và Truyền thông trong công tác đánh giá mức độ bảo đảm an toàn thông tin mạng;

c) Tăng cường tham gia các mạng lưới an toàn, an ninh mạng trong nước và các hoạt động, diễn đàn, tổ chức, mạng lưới quốc tế về an toàn, an ninh mạng theo quy định của pháp luật.

11. Hiệp hội An toàn thông tin Việt Nam (VNISA) có trách nhiệm:

a) Định kỳ hàng năm tổ chức khảo sát, đánh giá bình chọn và tôn vinh giải pháp, dịch vụ an toàn thông tin mạng Việt Nam tiêu biểu, chất lượng cao;

b) Chủ trì và phối hợp với các doanh nghiệp kinh doanh trong lĩnh vực an toàn thông tin mạng đề xuất tiêu chí và triển khai các biện pháp hỗ trợ nâng cao chất lượng sản phẩm, dịch vụ, nguồn nhân lực an toàn thông tin theo chuẩn quốc tế.

12. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet (ISP) có trách nhiệm:

a) Thiết lập, kiện toàn đầu mối đơn vị chuyên trách an toàn thông tin mạng trực thuộc để bảo vệ hệ thống, khách hàng của mình; tham gia hỗ trợ các cơ quan, tổ chức nhà nước giám sát, bảo vệ, kiểm tra, đánh giá an toàn thông tin mạng dưới sự điều phối của Bộ Thông tin và Truyền thông;

b) Triển khai các biện pháp kỹ thuật bảo vệ trẻ em trên môi trường mạng theo hướng dẫn của Bộ Thông tin và Truyền thông.

13. Tổ chức thực hiện:

a) Các Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương, Thủ trưởng các cơ quan, đơn vị và các tổ chức, cá nhân liên quan có trách nhiệm chỉ đạo và thi hành nghiêm Chỉ thị này;

LuatVietnam
Tiện ích văn bản luật

b) Đề nghị Văn phòng Trung ương và các Ban của Đảng, Văn phòng Quốc hội, Văn phòng Chủ tịch nước, Viện kiểm sát nhân dân tối cao, Tòa án nhân dân tối cao, Kiểm toán nhà nước, các tổ chức chính trị - xã hội tăng cường công tác bảo đảm an toàn, an ninh mạng tổng thể trong cơ quan, tổ chức theo quy định của pháp luật về an toàn, an ninh mạng và các quy định khác có liên quan./.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các đoàn thể;
- Các tập đoàn kinh tế và tổng công ty nhà nước;
- Các ngân hàng thương mại Nhà nước;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- Các Tổ chức tín dụng, tài chính Nhà nước;
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, TTTH;
- Lưu: VT, KSTT (2). 140

THỦ TƯỚNG

Nguyễn Xuân Phúc

LuatVietnam
Tiện ích văn bản luật