STT	Người ký	Đơn vị	Thời gian ký	Ý kiến
1	TẬP ĐOÀN CÔNG NGHIỆP - VIỄN THÔNG QUÂN ĐỘI		25/08/2022 14:02:37	Đã đóng dấu
2	TÀO ĐỨC THẮNG	Tổng giám đốc - Tập đoàn Công nghiệp - Viễn thông Quân đội	25/08/2022 11:34:24	

TẬP ĐOÀN CÔNG NGHIỆP-VIỄN THÔNG QUÂN ĐỘI

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 4396/CT-CNVTQĐ

Hà Nội, ngày 25 tháng 8 năm 2022

CHỈ THỊ
Về việc rà soát, tăng cường kiểm soát truy cập Internet tại các cơ quan, đơn vị thuộc Tập đoàn

Căn cứ Quy chế quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Tập đoàn Công nghiệp – Viễn thông Quân đội ban hành kèm theo Quyết định số 4631/QĐ-CNVTQĐ ngày 30/11/2020;

Căn cứ chỉ đạo của Tổng Giám đốc Tập đoàn Công nghiệp – Viễn thông Quân đội (CNVTQĐ),

Nhằm mục đích kịp thời khắc phục các nguy cơ mất an toàn thông tin, an ninh mạng, Tổng Giám đốc Tập đoàn chỉ thị:

1. Các cơ quan, đơn vị thuộc Tập đoàn

- Tăng cường công tác tuyên truyền, phổ biến giáo dục cán bộ, nhân viên nhằm nâng cao ý thức trong bảo đảm an toàn thông tin, an ninh mạng. Nâng cao hiệu lực, hiệu quả lãnh đạo, chỉ đạo các cấp, gắn trách nhiệm người đứng đầu cơ quan, đơn vị trong tổ chức triển khai và thực hiện nhiệm vụ về an toàn thông tin, an ninh mạng. Người đứng đầu cơ quan, đơn vị chịu trách trước Tổng Giám đốc Tập đoàn và pháp luật về các vi phạm, sự cố, vụ việc mất an toàn thông tin, an ninh mạng xảy ra tại đơn vị mình.

- Tổ chức rà soát, triển khai tuân thủ nghiêm Tiêu chuẩn an toàn thông tin trên máy tính người dùng cuối TC.CNVTQĐ.CNTT.09 và Tiêu chuẩn an toàn thông tin cho mạng Office số TC.CNVTQĐ.CNTT.13. ***Đặc biệt chú ý các nội dung tại Phụ lục I kèm theo***.

- Triển khai giải pháp kiểm soát truy cập Internet tập trung Web Security Gateway (WSG) do Công ty An Ninh mạng Viettel (VCS) cung cấp hoặc tương đương. Yêu cầu thiết lập tuân thủ đầy đủ Tiêu chuẩn an toàn thông tin cho hệ thống Proxy số TC.CNVTQĐ.CNTT.10 và ***bổ sung*** thêm các yêu cầu sau:

+ Chỉ mở truy nhập Internet theo danh sách được phép *(Whitelist)* cho đối tượng/nhóm đối tượng có nhu cầu *(Nhưng không được vi phạm chính sách tại Mục VI Khoản 4 của Tiêu chuẩn số TC.CNVTQĐ.CNTT.10)*. Mặc định chặn toàn bộ. ***Danh sách Whitelist phải được chỉ huy, lãnh đạo cao nhất của cơ quan, đơn vị phê duyệt bằng văn bản***.

+ Chặn kết nối từ máy chủ kiểm soát Internet tập trung đến các hệ thống, dịch vụ cho phép gửi/nhận, trao đổi thông tin, tài liệu, tệp dưới bất kỳ hình thức nào, như: WhatApp, Zalo, Telegram, Facebook Messenger,...

- Triển khai giải pháp kiểm soát truy cập mạng máy tính nội bộ NAC (Network Access Control) để quản lý các thiết bị đầu cuối, máy tính người dùng kết nối vào mạng máy tính. Ưu tiên lựa chọn giải pháp NAC do VCS cung cấp.

- Nghiên cứu, lập Kế hoạch triển khai giải pháp Remote Browser *(điều khiển trình duyệt từ xa, trình duyệt ảo)* hoặc máy tính VDI riêng biệt cho nhóm CBNV có nhu cầu tìm kiếm, tra cứu thông tin trên mạng Internet phục vụ công việc: Thiết lập chính sách chặn trao đổi dữ liệu giữa máy tính nội bộ với Remote Browser/máy tính VDI riêng biệt.

- Tổ chức quản lý và kiểm soát chặt chẽ các vật mang tin, thiết bị lưu trữ di động theo quy định tại Điều 25 của Quyết định số 4631/QĐ-CNVTQĐ.

- Tổ chức quán triệt và yêu cầu CBNV khi sử dụng thiết bị máy tính do cá nhân trang bị *(PC, laptop, Surface, Ipad, máy tính bảng khác,..),* điện thoại thông minh và các thiết bị lưu trữ dữ liệu di động do cá nhân trang bị *(Thẻ nhớ, USB, ổ cứng ngoài, băng từ,...)* để xử lý công việc của cơ quan, đơn vị phải có trách nhiệm bảo vệ các thiết bị và thông tin lưu trữ trên thiết bị đó, tránh làm mất, lộ lọt thông tin. Thực hiện xóa thông tin lưu trữ trên các thiết bị ngay sau khi hoàn thành công việc.

- Yêu cầu hoàn thành và báo cáo kết quả về Ban CNTT Tập đoàn **trước ngày 30/8/2022**.

2. Ban Hành chính Tập đoàn

- Giao đầu mối IT hành chính chủ trì tổ chức triển khai tuân thủ các yêu cầu tại Mục 1 của Chỉ thị này cho máy tính, mạng máy tính và hệ thống WSG của Khối Cơ quan Tập đoàn.

3. Ban Công nghệ Thông tin Tập đoàn

- Chủ trì phối hợp với Công ty An Ninh mạng Viettel kiểm tra định kỳ hoặc đột xuất việc tuân thủ Chỉ thị này tại các cơ quan, đơn vị thuộc Tập đoàn.

4. Công ty An Ninh mạng Viettel

- Sẵn sàng cung cấp sản phẩm, dịch vụ an toàn thông tin, an ninh mạng cho các đơn vị có nhu cầu *(như: EDR/EDP, NAC, WSG,..)*.

- Duy trì công tác giám sát an toàn thông tin, an ninh mạng theo chế độ 24x7. Liên tục cải tiến, bổ sung tính năng cho các sản phẩm, giải pháp SOC nhằm phát hiện sớm các vi phạm, lỗ hổng và sự cố an toàn thông tin, an ninh mạng xảy ra trên các hệ thống thông tin của các cơ quan đơn vị thuộc Tập đoàn.

- Phối hợp với Ban CNTT thực hiện kiểm tra định kỳ hoặc đột xuất việc tuân thủ Chỉ thị này tại các cơ quan, đơn vị thuộc Tập đoàn.

Chỉ thị này có hiệu lực từ ngày ký. Các cơ quan, đơn vị có tên trên chịu trách nhiệm thi hành ./.

Nơi nhận:
- Ban TGĐ TĐ (để b/c);
- Các cơ quan, đơn vị;
- Lưu: VT, CNTT. Khải 6.

TỔNG GIÁM ĐỐC

Đại tá Tào Đức Thắng

Phụ lục I:
CÁC NỘI DUNG ĐẶC BIỆT CHÚ Ý

1. Bảo đảm an toàn thông tin, an ninh mạng trên máy tính

TT	Yêu cầu	Tham chiếu tiêu chuẩn TC.CNVTQĐ.CNTT.09
1.	Các phần mềm, ứng dụng ***không được phép*** cài đặt trên máy tính: - Các phần mềm chat client (ví dụ: yahoo messenger, skype, google talk, msn chat, zalo, whatapp,viber,... hoặc các phần mềm tương đương). - Các phần mềm vượt tường lửa, proxy như các phần mềm proxy, vpn, tunnel (ví dụ: hostspot shield, ultrasurf hoặc các phần mềm tương đương). Trường hợp sử dụng phần mềm VPN (SVP/MSuite) phục vụ công việc cần sự chấp thuận có thời hạn của bộ phận ATTT/CNTT, lãnh đạo đơn vị phê duyệt và chịu trách nhiệm. - Các phần mềm bên ngoài cho phép remote, điều khiển máy tính từ xa (ví dụ: teamviewer, logmein, vnc, radmin, x-manager hoặc các phần mềm tương đương). Với trường hợp cần sử dụng phần mềm để remote phục vụ việc hỗ trợ khách hàng cần sự chấp thuận có thời hạn của bộ phận ATTT/CNTT, lãnh đạo/chỉ huy đơn vị phê duyệt và chịu trách nhiệm.	Phần V mục III khoản 2
2.	Kiểm soát truy cập: - Máy tính phải được kết nối (join domain) vào hệ thống Active Directory để quản lý chính sách tập trung về tài khoản, quyền truy cập,… - Giới hạn đăng nhập tài khoản người dùng trên máy join domain. Mỗi tài khoản người dùng chỉ được đăng nhập vào máy tính được cho phép (không được phép đăng nhập chéo trên máy khác). - Tắt tính năng truy cập, sử dụng máy tính từ xa (remote, remote desktop) qua mạng máy tính. Ngoại trừ các trường hợp được Ban CNTT thẩm định cho phép sử dụng (mở cho phép remote làm việc từ xa qua SVP/MSuite). - Máy tính được phép kết nối Internet phải đi qua hệ thống giám sát, kiểm soát tập trung (WSG, Proxy Server,..). Đối với máy tính đối tác Out Source cần	Phần V mục III khoản 5 điểm d, i, j, m, o

TT	Yêu cầu	Tham chiếu tiêu chuẩn TC.CNVTQĐ.CNTT.09
	quy hoạch vào VLAN riêng; chặn toàn bộ kết nối, chỉ mở kết nối đến hệ thống chứa source code tập trung, hệ thống test theo quy định. Trường hợp cần mở truy cập một số web phục vụ công việc phải truy cập qua WSG, whitelist các địa chỉ cần sử dụng; chặn tính năng upload và được sự phê duyệt của bộ phận ATTT/CNTT đơn vị, có thời hạn. - Với nhóm máy tính đối tác thuê ngoài (outsource): chỉ cho phép kết nối đến các nhóm máy chủ chứa source code tập trung (SVN, Git, IBM…); máy chủ test nghiệp vụ; và các máy chủ cần thiết phục vụ cho công việc đã được bộ phận ATTT đơn vị thẩm định (server chat).	
3.	Phòng chống phần mềm độc hại và giám sát an toàn thông tin: - Máy tính phải cài đặt phần mềm giám sát ATTT (Endpoint Security/OneAgent/EDR) do VCS cung cấp. - Cài đặt phần mềm Antivirus: Thiết lập cấu hình update định kỳ tối thiểu 1 ngày 1 lần; Thiết lập cấu hình quét toàn bộ theo tối thiểu 1 tháng 1 lần; Luôn bật chức năng realtime protection.	Phần V mục III khoản 8
4.	Bảo đảm an toàn dữ liệu: - Thiết lập chế độ chặn truy cập, sử dụng các thiết bị lưu trữ, đọc ghi dữ liệu (USB, Ổ cứng di động, ổ đĩa CD, DVD, ...) kết nối với máy tính. - Chặn trao đổi dữ liệu qua giao thức truy nhập từ xa vào máy tính. - Chặn trao đổi dữ liệu (gửi/nhận) giữa máy tính ở nhà với máy tính ở Cơ quan, đơn vị phục vụ cho mục đích làm việc từ xa (bao gồm cả clipboard, Drivers, printer,…) - Cài đặt sử dụng phần mềm quản lý văn bản mật do VCS cung cấp. Các dữ liệu mật, tài liệu mật, quan trọng theo quy định Công tác bảo vệ bí mật Nhà nước trong Tập đoàn Công nghiệp – Viễn thông Quân Đội (Số 2964/QĐ-CNVTQĐ) cần được lưu trữ trong thư mục, phân vùng mật.	Phần V mục III khoản 9 điểm a, b, c, e, f,g

TT	Yêu cầu	Tham chiếu tiêu chuẩn TC.CNVTQĐ.CNTT.09
	- Khuyến nghị sử dụng tính năng mã hóa phân vùng ổ cứng Bitlocker trên Hệ điều hành Windows để bảo vệ dữ liệu. - CBNV sử dụng máy tính cá nhân và các thiết bị lưu trữ dữ liệu di động (thẻ nhớ, USB, ổ cứng ngoài, băng từ,...) để xử lý công việc của Tập đoàn có trách nhiệm bảo vệ các thiết bị và thông tin lưu trữ trên các thiết bị đó, tránh làm mất, lộ lọt thông tin; Thực hiện xóa thông tin lưu trữ trên các thiết bị lưu trữ dữ liệu di động ngay sau khi hoàn thành công việc.	

2. Thiết lập chính sách ATTT trên hệ thống kiểm soát truy nhập Internet tập trung

TT	Yêu cầu	Tham chiếu Tiêu chuẩn TC.CNVTQĐ.CNTT.10
1.	Thực hiện xác thực người dùng khi sử dụng Proxy *(Khuyến nghị tích hợp xác thực với hệ thống Active Directory)*;	Mục VI. Khoản 4
2.	Khuyến nghị cấu hình máy tính người dùng sử dụng file Proxy.pac;	
3.	Giới hạn chỉ mở cho dải IP người dùng được phép truy cập Proxy;	
4.	Giới hạn các cổng Internet mà người dùng truy cập, mặc định chỉ mở cổng 80, 443. Trong trường hợp cần mở thêm thì chỉ mở thêm những cổng cần thiết, không mở tất cả cổng *(Phải được thẩm định bởi bộ phận ATTT/CNTT, và phê duyệt của Lãnh đạo/chỉ huy đơn vị)*;	
5.	Thực hiện chặn kết nối đến các máy chủ điều khiển từ xa *(Teamviewer, Logmein, Ultraviewer)*.	
6.	Thực hiện chặn người dùng upload tài liệu lên các trang chia sẻ dữ liệu trực tuyến, truy cập public email, mạng xã hội.	