

Số: 13 /STTTT-CNTT  
V/v cảnh báo mối nguy tấn công vào  
dịch vụ SSH

Bến Tre, ngày 28 tháng 6 năm 2010

SỞ GIÁO DỤC VÀ ĐÀO TẠO BẾN TRE	
<b>ĐẾN</b>	Số: 1149
	Ngày: 29/6
Chuyển: .....	

Kính gửi:

- Sở, Ngành tỉnh;
- Ủy ban nhân dân các huyện, thành phố;

Theo tinh thần công văn số 129/VNCERT-NV ngày 21 tháng 6 năm 2010 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam về việc cảnh báo mối nguy tấn công vào dịch vụ SSH, Sở Thông tin và Truyền thông trân trọng thông báo đến Quý cơ quan biết và khuyến cáo một số biện pháp kỹ thuật sau để hạn chế nguy cơ bị mất kiểm soát hệ thống thông tin:

1. Thay đổi công hoạt động mặc định của dịch vụ SSH (nếu có thể mặc định là công 22).
2. Phát hiện và ngăn chặn các dấu hiệu tấn công brute-force vào dịch vụ SSH: đăng nhập nhiều lần liên tiếp vào một hoặc nhiều tài khoản với mật khẩu không chính xác. Giới hạn tần suất đăng nhập nếu có thể.
3. Không cho phép đăng nhập trực tiếp vào tài khoản quản trị (root, administrator) qua SSH.
4. Thay đổi cơ chế xác thực đăng nhập, dùng khóa cá nhân (private key) thay cho mật khẩu (password). Trong trường hợp buộc phải dùng cơ chế đăng nhập bằng mật khẩu thì đảm bảo mật khẩu phải an toàn, bí mật.
5. Giới hạn chỉ cho phép những tài khoản cần thiết được đăng nhập vào dịch vụ SSH.
6. Cần nhắc sử dụng thiết lập "chroot" để giới hạn các thư mục được phép truy xuất.
7. Giới hạn các địa chỉ IP được kết nối và đăng nhập vào dịch vụ SSH.

Ngoài ra, Quý cơ quan có thể theo dõi trên website của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) tại địa chỉ:

<http://vncert.gov.vn/canhbao/cbnd/CBND10-002.htm>

Thông tin liên hệ: Trung tâm VNCERT (Ông: Kiều Minh Thắng, Điện thoại: 0913.525.274 hoặc 04-3640.4424, Fax: 04-3460.4425)

Trân trọng./.

Nơi nhận:

- Như trên;
- Các Phòng VH TT;
- Lưu CNTT, VT.

