**Các cuộc tấn công:**

1. Vụ hệ thống mạng Tổng công ty cổ phần Bảo hiểm bưu điện (PTI) và Chứng khoán VNDirect bị tấn công cùng thời điểm được nhận định có thể là do dùng chung hệ thống quản lý máy chủ mạng.



*Sàn giao dịch chứng khoán VNDirect trước khi bị tấn công*

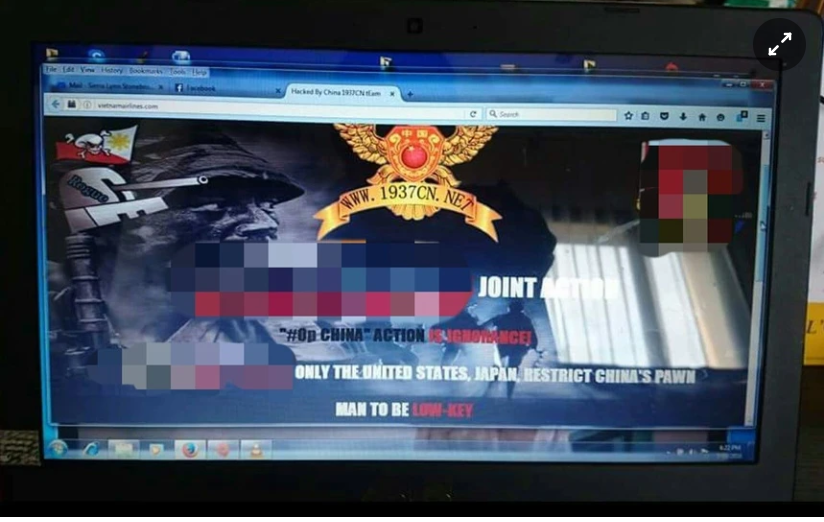
2. Năm 2022: Hacker có bí danh "ChinaDan" rao bán dữ liệu được cho là rỏ rì từ Sở Cảnh sát Quốc gia Thượng Hải trên một diễn đàn dành cho hacker



*Bài rao bán dữ liệu của thành viên ChinaDan trên diễn đàn hacker.*

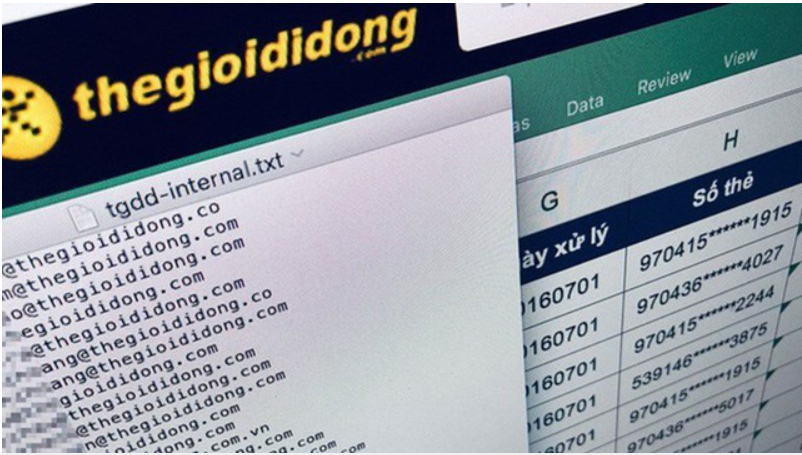
3. Ở Việt Nam

* + Lộ lọt thông tin 400.000 khách hàng của Vietnam Airlines năm 2017;



Website của Vietnam Airlines bị tin tặc tấn công.

* + Lộ lọt thông tin của 5 triệu khách hàng Thế giới di động năm 2018;

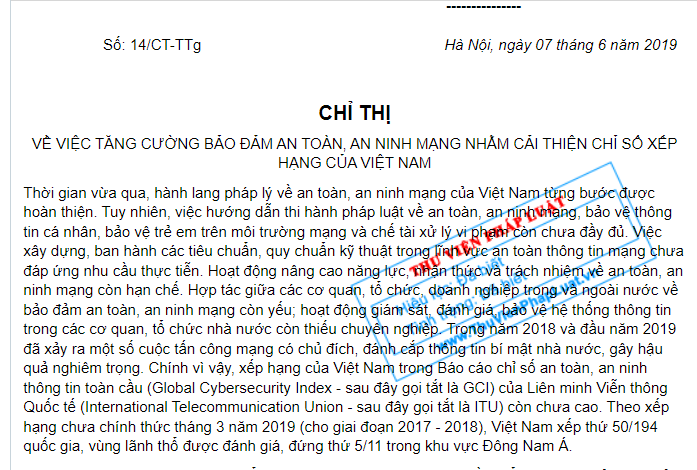


*Vấn đề bảo mật thông tin cá nhân đang trở nên cấp bách.*

* + Rao bán thông tin 5 triệu người dùng ô tô Việt Nam trên chợ đen (tháng 9/2021).

## 1 Hệ thống phòng thủ 4 lớp

Đây là hệ thống nhằm bảo đảm an toàn thông tin mạng được Thủ tướng Chính phủ chỉ đạo thực hiện tại[Chỉ thị 14/CT-TTg](https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Chi-thi-14-CT-TTg-2019-bao-dam-an-toan-an-ninh-mang-cai-thien-chi-so-xep-hang-cua-Viet-Nam-416078.aspx" \t "_blank) ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.



*Chỉ thị 14/CT-TTg*

Mô hình này được Bộ Thông tin và Truyền thông hướng dẫn thực hiện tại:[Công văn 1552/BTTTT- CATTT](https://thuvienphapluat.vn/cong-van/Cong-nghe-thong-tin/Cong-van-1552-BTTTT-CATTT-2020-to-chuc-trien-khai-bao-dam-an-toan-cho-he-thong-thong-tin-theo-4-lop-451553.aspx) ngày 28/4/2020 về việc đôn đốc tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin theo mô hình “4 lớp”



[*Công văn 1552/BTTTT- CATTT*](https://thuvienphapluat.vn/cong-van/Cong-nghe-thong-tin/Cong-van-1552-BTTTT-CATTT-2020-to-chuc-trien-khai-bao-dam-an-toan-cho-he-thong-thong-tin-theo-4-lop-451553.aspx)

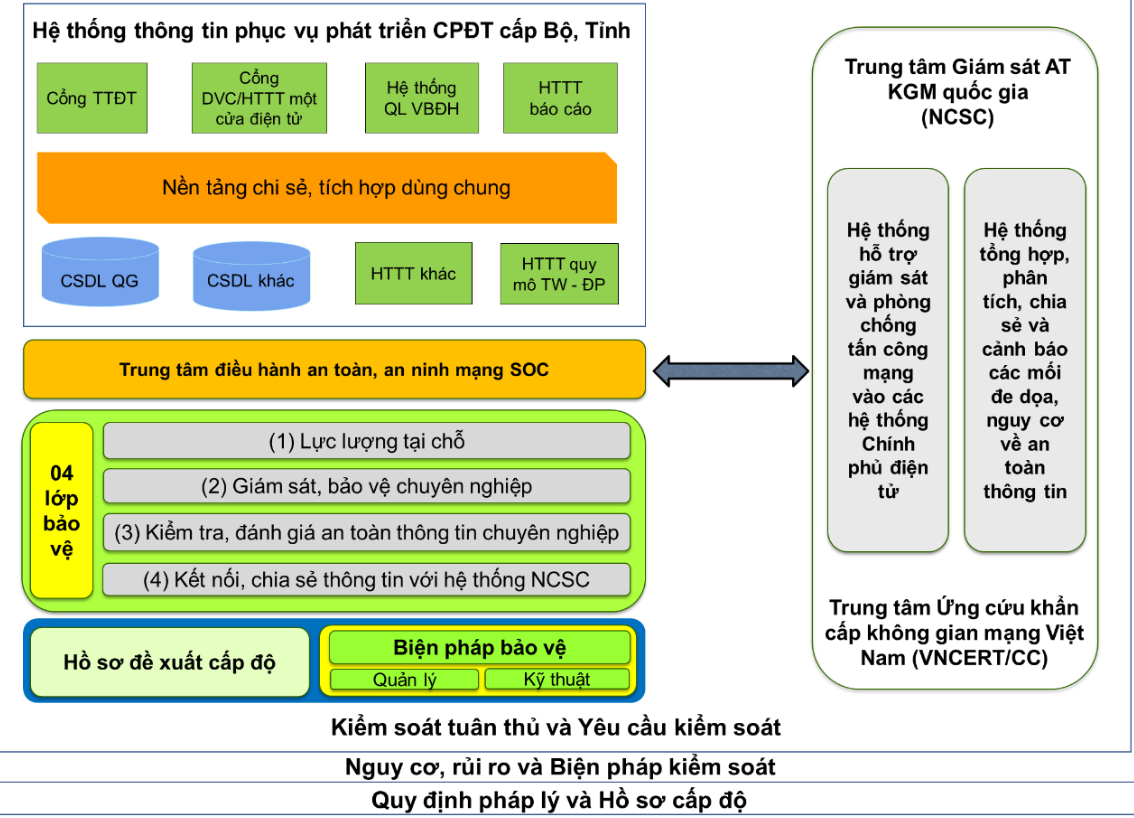
Hệ thống phòng thủ 4 lớp về chính sách bao gồm:

Lớp 1: Lực lượng tại chỗ

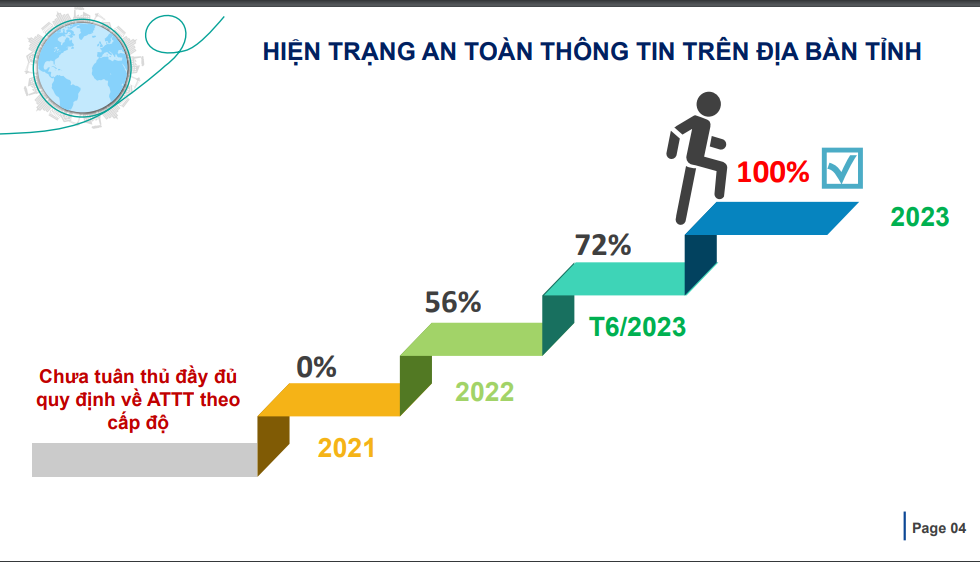
Lớp 2 Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp

Lớp 3: Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ

Lớp 4: Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia



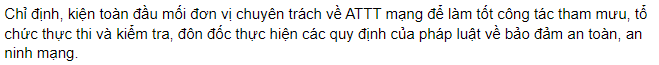
*Mô hình bảo đảm an toàn thông tin cấp bộ, tỉnh*



*Hiện trạng ATTT trên địa bàn tỉnh*

* **Yêu cầu về ATTT theo mô hình 4 lớp:**

**Lớp 1: Lực lượng tại chỗ**

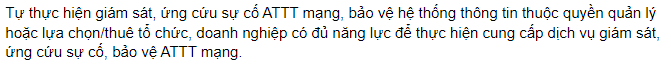
****

Gồm bộ phận chuyên trách về an toàn thông tin (BĐPT ATTT) và cán bộ, nhân viên được đào tạo về an toàn thông tin.

**Có trách nhiệm thực hiện** các công việc như:

* Quản lý, vận hành hệ thống thông tin an toàn.
* Giám sát, phát hiện và xử lý vi phạm an ninh mạng.
* Nâng cao nhận thức về an toàn thông tin cho cán bộ, nhân viên.
* Phối hợp với các cơ quan, tổ chức khác trong công tác bảo đảm an toàn thông tin.

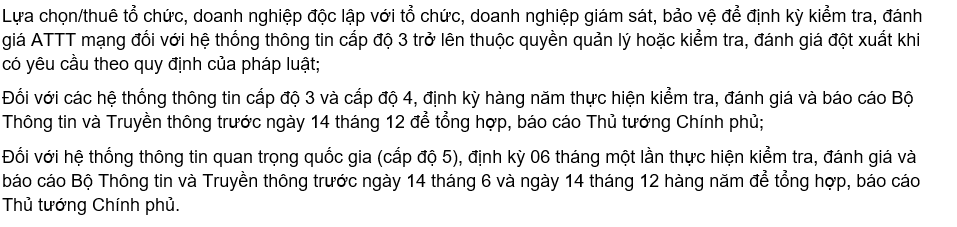
**Lớp 2: Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp**

****

**Có trách nhiệm** thực hiện các công việc như:

* Giám sát an ninh mạng 24/7.
* Phân tích và cảnh báo các mối đe dọa an ninh mạng.
* Ứng phó sự cố an ninh mạng.
* Thực hiện cá+c hoạt động kiểm tra, đánh giá an ninh mạng định kỳ.

**Lớp 3: Tổ chức hoặc thuê doanh nghiệp độc lập, đánh giá định kỳ**

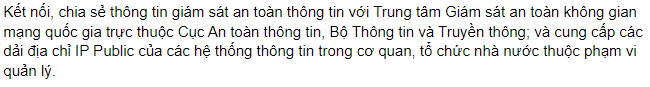


Là các tổ chức cung cấp dịch vụ giám sát, bảo vệ hệ thống thông tin.

**Có trách nhiệm** thực hiện các công việc như:

* Giám sát an ninh mạng 24/7.
* Phân tích và cảnh báo các mối đe dọa an ninh mạng.
* Ứng phó sự cố an ninh mạng.
* Thực hiện các hoạt động kiểm tra, đánh giá an ninh mạng định kỳ.

**Lớp 4: Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia**

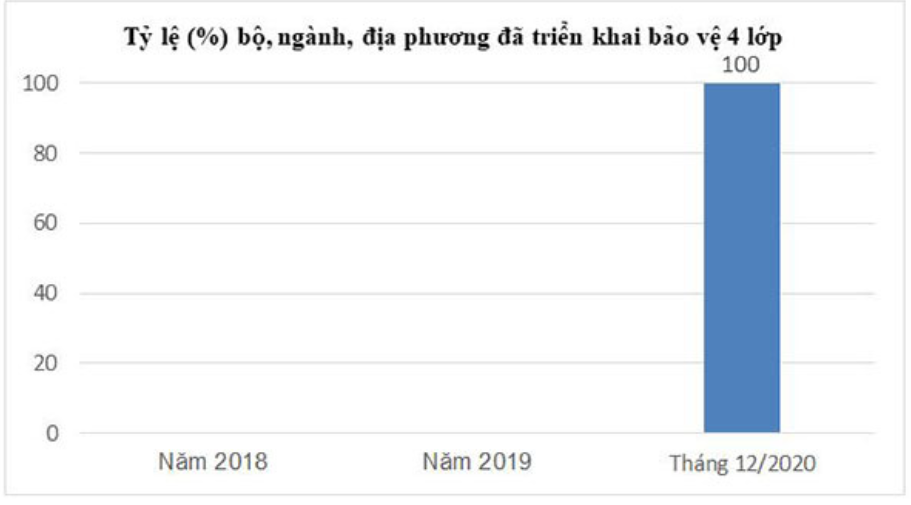
****

Gồm Trung tâm Giám sát an ninh mạng quốc gia (VNCert) và các hệ thống giám sát an ninh mạng khác.

Theo công bố của Bộ TT&TT hồi đầu tháng 7/2020, đã có 8 doanh nghiệp gồm: **Viettel, VNPT, BKAV, FPT IS, CMC Cyber Security, CyRadar, VNCS Global** và **SAVIS** cung cấp nền tảng dịch vụ SOC đáp ứng yêu cầu kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia.

**Có trách nhiệm** thực hiện các công việc như:

* Thu thập, chia sẻ thông tin về các mối đe dọa an ninh mạng.
* Phân tích và cảnh báo các mối đe dọa an ninh mạng trên diện rộng.
* Hỗ trợ các cơ quan, tổ chức trong công tác bảo đảm an toàn thông tin.
* Mô hình phòng thủ 4 lớp giúp cho việc bảo đảm an toàn thông tin được thực hiện một cách hiệu quả, toàn diện, góp phần bảo vệ hệ thống thông tin quốc gia trước các nguy cơ tấn công mạng ngày càng gia tăng.
* **Ngoài 4 lớp chính, mô hình phòng thủ còn có thể bao gồm các lớp bổ sung khác như:**
* Lớp quản lý: Ban hành các chính sách, quy định về an toàn thông tin.
* Lớp giáo dục, đào tạo: Nâng cao nhận thức về an toàn thông tin cho cán bộ, nhân viên.
* Lớp công nghệ: Triển khai các giải pháp công nghệ bảo mật tiên tiến.



*Tỷ lệ (%) bộ, ngành, địa phương đã triển khai bảo vệ 4 lớp*

* **Mục tiêu thực hiện mô hình “4 lớp”**

Đối với việc thực hiện mô hình này, Bộ Thông tin và Truyền thông đã đưa ra mục tiêu 100% hệ thống thông tin của cơ quan, tổ chức được tổ chức bảo đảm an toàn thông tin một cách toàn diện, thực chất theo hướng dẫn của Bộ. Bên cạnh đó, phải đòi hỏi nâng cao năng lực của lớp giám sát, bảo vệ chuyên nghiệp và kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

* **Giải pháp thực hiện mô hình “4 lớp”**
* Nâng cao năng lực lực lượng tại chỗ đáp ứng yêu cầu mới thông qua đào tạo, tuyển dụng hoặc thuê chuyên gia, bảo đảm mỗi đơn vị chuyên trách an toàn thông tin có tối thiểu 05 chuyên gia an toàn thông tin mạng.
* Hoàn thành mở rộng phạm vi giám sát, bảo vệ cho 100% hệ thống thông tin thuộc phạm vi quản lý chậm nhất trong tháng 11/2024. Đối với các hệ thống thông tin cấp độ 3 trở lên, khuyến nghị tổ chức giám sát, bảo vệ đầy đủ các lớp: lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu, lớp thiết bị đầu cuối.
* Kiểm tra, đánh giá an toàn thông tin định kỳ theo quy định cho hệ thống thông tin thuộc phạm vi quản lý. Rà soát danh sách các webiste (.gov.vn) bao gồm cả các sub domain để tiến hành đánh giá an toàn thông tin định kỳ và triển khai gán nhãn tín nhiệm mạng cho các webiste.
* Duy trì kết nối ổn định, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực về Hệ thống giám sát quốc gia để được hỗ trợ giám sát, phân tích, cảnh báo sớm các nguy cơ về an toàn thông tin mạng và tấn công mạng.
* Thay đổi tư duy từ phát triển các hệ thống thông tin, phần mềm riêng lẻ sang đầu tư các nền tảng số hoặc thuê mua các dịch vụ do các doanh nghiệp cung cấp hạ tầng đã triển khai đầy đủ giải pháp bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình “4 lớp”.