Nâng cao năng lực quản trị không gian mạng

Kiểm soát rủi ro an toàn, an ninh thông tin trên không gian mạng

NỘI DUNG CHÍNH

01 Hiện trạng các rủi ro trên không gian mạng (KGM)

02 Giải pháp Viettel áp dụng để hạn chế rủi ro KGM

1. Hiện trạng các rủi ro trên không gian mạng

Vấn đề lộ lọt dữ liệu cá nhân

Dữ liệu cá nhân của 2/3 dân số nước ta đang được lưu trữ, đăng tải, chia sẻ và thu thập trên không gian mạng với nhiều hình thức, mức độ khác nhau.

- Vừa qua, hơn 163 triệu thông tin tài khoản của khách hàng công ty VNG bị lộ.
- Công ty Thế giới di động và điện máy xanh cũng từng để lộ hơn 5 triệu Email và hàng chục nghìn thông tin thẻ thanh toán của khách hàng.
- Vietnam Airlines đã bị tin tặc tấn công và đăng tải lên internet 411.000 tài khoản khách hàng thành viên của chương trình Bông Sen Vàng.

Dữ liệu của 30 triệu hồ sơ người dùng gồm đầy đủ tên, số điện thoại, địa chỉ Email, tài khoản đăng nhập và 360.000 thông tin của sinh viên Việt Nam được thu thập từ một trang web giáo dục trực tuyến được rao bán công khai trên mạng

Nguồn: *Báo cáo của Bộ CA tại phiên họp thứ 14 của Ủy ban Thường vụ Quốc hội.*

1. Hiện trạng các rủi ro trên không gian mạng

1. Khách hàng công khai thông tin cá nhân trên mạng thông qua giao dịch thương mại điện tử, tham gia trò chơi trực tuyến cũng như khi truy cập trang quảng cáo trên các website

2. Thông tin đăng ký và trong quá trình sử dụng các trang mạng xã hội như Facebook, Ticktok, Zalo, Instagram…

3. Sử dụng các ứng dụng di động, game di động, ứng dụng bói toán/hẹn hò… và đồng ý các điều khoản cấp quyền truy cập dữ liệu (như danh sách bạn bè trên Facebook, hồ sơ cá nhân…), các ứng dụng trên mobile theo dõi hành vi người dùng…

4. Lộ lọt từ các lỗ hổng trong công tác bảo mật dữ liệu, an toàn thông tin của nhà cung cấp dịch vụ.

1. Hiện trạng các rủi ro trên không gian mạng

Rủi ro về lừa đảo trên mạng

Năm 2022 đã ghi nhận hơn 12.935 trường hợp lừa đảo trực tuyến, với 2 loại hình lừa đảo chính:

- Lừa đảo để đánh cắp thông tin cá nhân (chiếm 24.4%) và lừa đảo tài chính (chiếm 75,6%).
- Việc lừa đảo đánh cắp thông tin cá nhân cũng là bước đệm để tiếp nối cho việc lên kịch bản thực hiện lừa đảo tài chính.

➔ Mục tiêu cuối cùng đều là lừa đảo chiếm đoạt tài sản. Đều đánh chung vào tâm lý nhẹ dạ cả tin, thiếu sự tiếp cận thông tin, thiếu việc làm hoặc thu nhập thấp, đánh vào lòng tham của con người.

Nguồn: https://baochinhphu.vn/

1. Hiện trạng các rủi ro trên không gian mạng

Rủi ro về lừa đảo trên mạng

Các hình thức lừa đảo KH thông thường gồm:

- Giả mạo thương hiệu của các tổ chức (Ngân hàng, cơ quan nhà nước, công ty tài chính, chứng khoán…) để gửi SMS lừa đảo cho nạn nhân.
- Thông báo trúng thưởng, quà tặng, khuyến mại để lừa nạn nhân đánh cắp thông tin tài khoản và tài sản thông qua các trang web giả mạo.
- Thủ đoạn nâng cấp lên SIM 4G hay 5G để lừa lấy số điện thoại của nạn nhân nhằm chiếm đoạt thông tin tài khoản và tài sản.
- Giả mạo email của ngân hàng, ví điện tử, tổ chức uy tín để uy hiếp, đe doạ lừa tiền nạn nhân.
- Lập sàn đầu tư tiền ảo crypto, đầu tư đa cấp, đầu tư nhị phân, đầu tư Forex… lừa đảo chiếm đoạt tài sản.

1. Hiện trạng các rủi ro trên không gian mạng

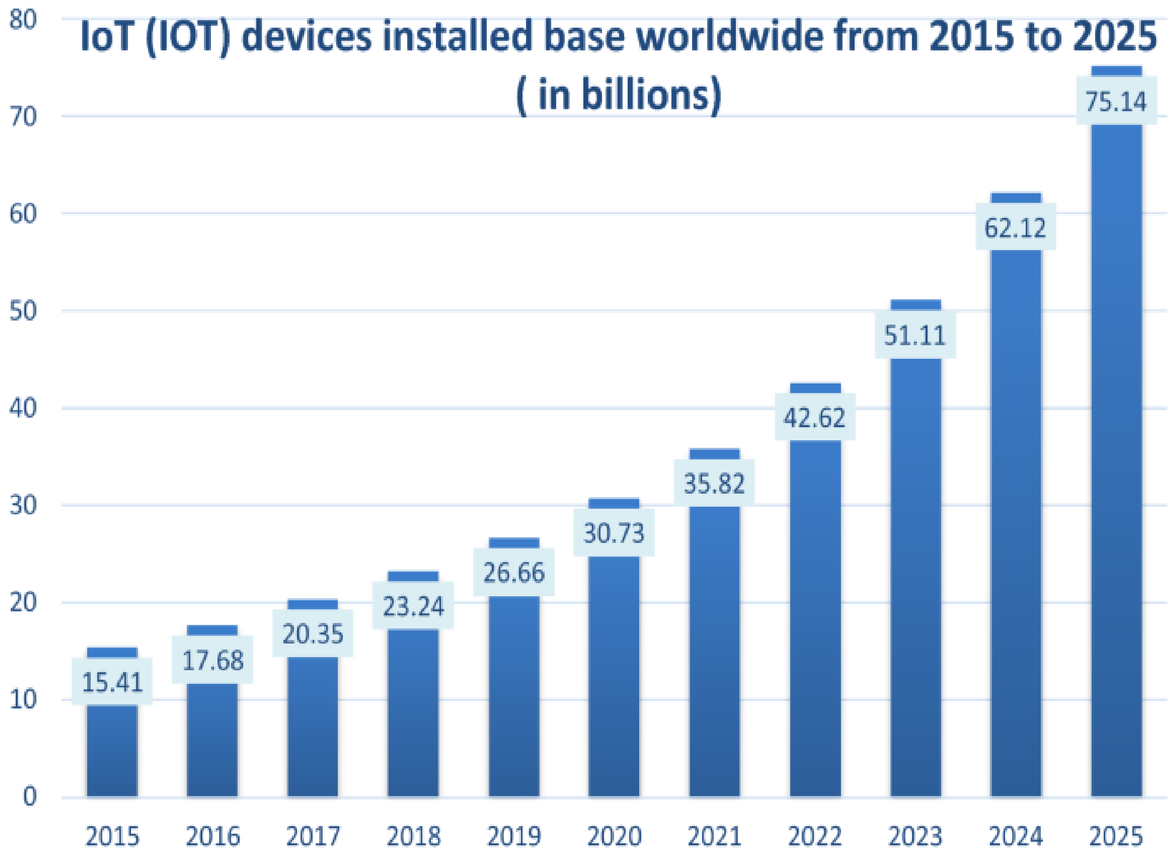
Rủi ro trên KGM với ISP

Tăng nguy cơ và thiệt hại do tấn công DDOS

Sự gia tăng nhanh chóng của thiết bị IoT trên thế giới

- Năm 2015 thế giới có 15 tỷ thiết bị IoT trên toàn thế giới
- Năm 2023 con số này là 51.11 tỉ, dự kiến năm 2025 thế giới có 75 tỉ thiết bị IoT được sử dụng.

Số lượng thiết bị **IoT** hiện nay trên TG và dự báo tăng trưởng



1. Hiện trạng các rủi ro trên không gian mạng

*Số lượng thiết bị **Camera CCTV** năm 2019*

Country	# of CCTV Cameras	# of People	# of CCTV Cameras per 100 People
United States	50 000 000	327,167,430	15.28
China	200 000 000	1,392,730,000	14.36
United Kingdom	5 000 000	66,488,990	7.5
Germany	5 200 000	82,927,920	6.27
Netherlands	1 000 000	17,231,020	5.80
Australia	1 000 000	24,992,370	4
Japan	5 000 000	126,529,100	3.95
Vietnam	2 600 000	95,540,400	2.72
France	1 650 000	66,987,240	2.46
South Korea	1 030 000	51,635,260	1.99

precisesecurity.com

Rủi ro trên KGM với ISP

Tăng nguy cơ và thiệt hại do tấn công DDOS

Tính đến hết năm 2019, về số lượng camera/ đầu người của một số nước có tỉ lệ cao nhất trên TG như sau:

- Mỹ là quốc gia có tỷ lệ này cao nhất với khoảng 15,3 camera/100 người.
- Trung Quốc, tỷ lệ này là 14,4 camera/100 dân.
- Tại khu vực châu Âu, Đức là quốc gia sở hữu nhiều camera nhất với tỷ lệ 6,3 camera/100 người, Anh là 7,5 camera /100 người và tại Nhật là 2,7 camera/100 người. *Có thể thấy các quốc gia phát triển trên thế giới đang rất tích cực ứng dụng camera trong việc giám sát và đảm bảo an ninh.*
- Đối với Việt Nam, hiện cả nước đang có khoảng 2,6 triệu camera an ninh. Tỷ lệ camera của nước ta là khoảng 2,6 camera/100 dân.

1. Hiện trạng các rủi ro trên không gian mạng

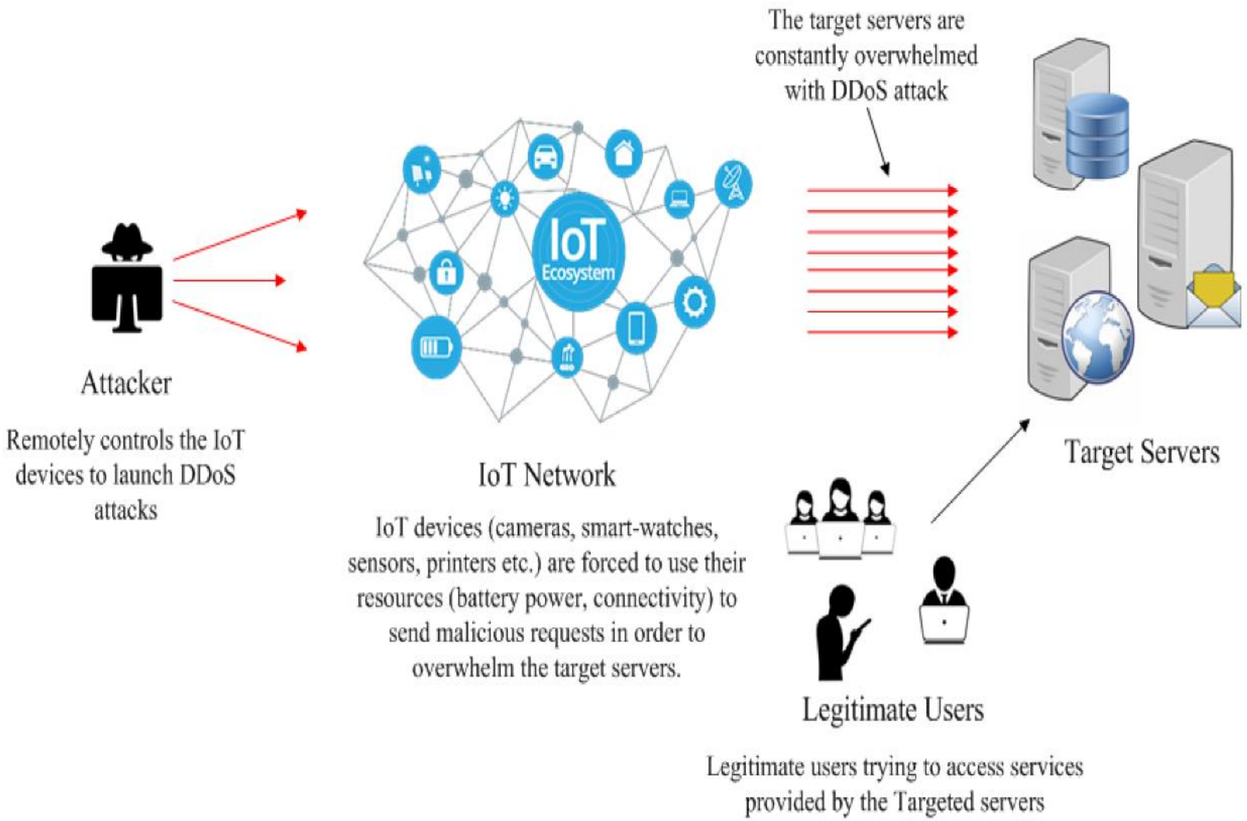
Rủi ro trên KGM với ISP

Nguy cơ của tấn công DDoS từ thiết bị IoT và Camera

Các ISP thông thường đã là mục tiêu ưa thích của các cuộc tấn công từ chối dịch vụ ở quy mô lớn. Khi thiết bị IoT, CCTV tăng trưởng nhanh chóng, dẫn theo nguy cơ về quy mô và mức độ thiệt hại trong các cuộc tấn công DDoS càng trở nên nghiêm trọng hơn.

Nguy cơ lộ dữ liệu cá nhân từ thiết bị IoT và Camera

- Số lượng thiết bị IoT và camera giám sát bùng nổ là ngoài việc làm gia tăng rủi ro tấn công DDoS vào hạ tầng của các ISP còn là nguồn gia tăng rủi ro về lộ thông tin cá nhân do thông tin thu thập được của các thiết bị này.
- Trường hợp các thiết bị IoT và camera không có tiêu chuẩn bảo mật nghiêm ngặt, dữ liệu sau khi thu thập được có thể đưa về cho nhà sản xuất và được sử dụng với mục đích chủ thể dữ liệu không hay biết hoặc cũng có thể bị tin tặc dễ dàng chiếm quyền khai thác, đánh cắp thông tin trên các hệ thống chứa dữ liệu quan sát.



1. Hiện trạng các rủi ro trên không gian mạng

Rủi ro trên KGM với ISP

Dịch vụ điện toán đám mây (Cloud service) cũng gia tăng nguy cơ rủi ro an ninh mạng đối với các ISP

- Theo Statista, hơn 53 triệu người ở Hoa Kỳ bị ảnh hưởng bởi hành vi xâm phạm, làm rò rỉ dữ liệu dữ liệu trong cùng một khoảng thời gian. Đây là một trong những rủi ro phổ biến nhất của điện toán đám mây.
- Theo một phân tích khác của Skyhigh, 21% tệp được tải lên Dịch vụ chia sẻ tệp dựa trên đám mây có chứa dữ liệu nhạy cảm. Khi một dịch vụ đám mây bị tấn công, tội phạm mạng sẽ có được quyền truy cập vào những dữ liệu nhạy cảm này. Kể cả khi không có vi phạm xảy ra, một số dịch vụ vẫn có thể ẩn chứa rủi ro rò rỉ một khi dữ liệu được tải lên.
- Khi dữ liệu của các cá nhân, tổ chức được đưa lên “mây” và lưu trữ trên hạ tầng đám mây của ISP, vấn đề luân chuyển dữ liệu xuyên biên giới rất khó kiểm soát. Hiện các luật của VN và nhiều nước trên thế giới đều có những quy định về việc lưu trữ dữ liệu của người dân, tổ chức của họ.
- Viettel hiện là nhà cung cấp dịch vụ điện toán đám mây hàng đầu Việt Nam về quy mô hạ tầng (dịch vụ Vcloud) đứng trước rất nhiều rủi ro về bảo mật khi dữ liệu của khách hàng đưa lên hạ tầng public cloud, các cơ chế chia sẻ trách nhiệm chưa rõ ràng sẽ khó quy trách nhiệm giữa ISP và khách hàng khi sự cố bảo mật dữ liệu xảy ra.

1. Hiện trạng các rủi ro trên không gian mạng

Rủi ro trong bối cảnh ra đời các luật về bảo vệ dữ liệu cá nhân hiện nay

Tình hình thế giới

- Các quốc gia trên thế giới đã và đang thắt chặt các chính sách, quy định về vấn đề bảo vệ dữ liệu người dùng, trong đó nổi bật lên là quy định của luật EU về bảo vệ dữ liệu và quyền riêng tư cho tất cả các cá nhân trong Liên minh châu Âu và Khu vực kinh tế châu Âu - The General Data Protection Regulation (GDPR) , Đạo luật bảo mật người tiêu dùng California (CCPA) *…yêu cầu các tổ chức, doanh nghiệp sử dụng dữ liệu bắt buộc phải có những cơ chế, chính sách, công cụ phù hợp để bảo vệ thông tin của người tiêu dùng*
- *Việc quản lý thông tin không tốt có thể gây tổn hại rất lớn cho các doanh nghiệp, tổ chức liên quan*. Facebook đã phải trả 500 nghìn bảng cho các vi phạm về dữ liệu sau khi GDPR có hiệu lực ; còn tại Mỹ, IBM ước tính tổng chi phí thiệt hại hàng năm của các doanh nghiệp liên quan đến vấn đề quản lý dữ liệu lên tới 3.1 nghìn tỷ đô la .

1. Hiện trạng các rủi ro trên không gian mạng

Rủi ro trong bối cảnh ra đời các luật về bảo vệ dữ liệu cá nhân hiện nay

Tại Việt Nam

- Sở hữu hạ tầng cung cấp dịch vụ di động và internet lớn nhất Việt Nam với hơn 60 triệu thuê bao khách hàng cá nhân và tổ chức, Viettel còn đứng trước rủi ro về pháp lý khi các luật/nghị định mới về an toàn thông tin, an ninh mạng, bảo vệ dữ liệu cá nhân (Luật An ninh mạng năm 2018; Nghị định 53/2022/NĐ-CP
- Ngày 17/4/2023, Chính phủ đã ban hành **Nghị định 13/2023/NĐ-CP** về bảo vệ dữ liệu cá nhân,có hiệu lực vào ngày 01/07/2023. Phạm vi điều chỉnh của Nghị định 13 đặt trọng tâm vào việc bảo vệ quyền của chủ thể dữ liệu và trách nhiệm của các đối tượng có hoạt động xử lý dữ liệu cá nhân → Tất cả các doanh nghiệp (bao gồm cả doanh nghiệp thu thập, lưu trữ dữ liệu cá nhân không nhằm mục đích kinh doanh) đều trở thành đối tượng của hoạt động xử lý dữ liệu cá nhân theo Nghị định 13/2023/NĐ-CP

➔ Các luật, nghị định ra đời là hành lang pháp lý rất chặt chẽ yêu cầu nhà mạng phải thay đổi đáng kể chính sách, công nghệ để đảm bảo các yêu cầu của luật.

2. Giải pháp Viettel áp dụng để hạn chế rủi ro KGM

Chính sách

- Xây dựng quy định nội bộ về bảo đảm an toàn hệ thống thông tin và an toàn dữ liệu dựa trên các quy định pháp luật.
- Căn cứ vào các quy định để xây dựng các bộ tiêu chuẩn, quy trình, quy chế, quy định ATTT và Quản trị dữ liệu
- Đinh kỳ kiểm tra, giám sát đảm bảo tính tuân thủ các chính sách đã được ban hành.

Công nghệ

- Phát triển, triển khai các giải pháp CNTT đảm bảo tuân thủ các chính sách đã được xây dựng. Đảm bảo bao phủ đầy đủ phạm vi từ hạ tầng mạng lưới, ứng dụng, mạng văn phòng và thiết bị đầu cuối.
- Triển khai DevSecOp, đưa quá trình đề xuất, đánh giá, thẩm định, phát triển các yêu cầu về ATTT của các hệ thống, ứng dụng ngay những bước đầu của SDLC và xuyên suốt quá trình VHKT hệ thống.

Con người

- Tổ chức bộ máy ATTT chuyên trách tại tất các đơn vị có chức năng PTPM hoặc VHKT HT CNTT.
- Đào tạo, kiểm tra định kỳ kiến thức về ATTT với các cấp quản lý, các lĩnh vực nghiệp vụ, đặc biệt các vai trò trong PTPM và VHKT HT CNTT.
- Tăng cường tuyên truyền, cảnh báo, nhắc nhở nhân viên và khách hàng ý thức về tự đảm bảo ATTTT.

XIN CẢM ƠN!