VNPT

TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG VIỆT NAM

CHUYÊN ĐỀ 4

CÁC GIẢI PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CÔNG CUỘC CHUYỂN ĐỔI SỐ NGÀNH CÔNG THƯƠNG

Bình Dương, 08/2024

NỘI DUNG

01 Thách thức về ATTT tại Việt Nam

02 Câu chuyện khách hàng

03 Chiến lược đảm bảo ATTT trong Chuyển đổi số

04 Năng lực, Giải pháp của VNPT trong lĩnh vực Cloud - ATTT

01

THÁCH THỨC VỀ ATTT TẠI VIỆT NAM

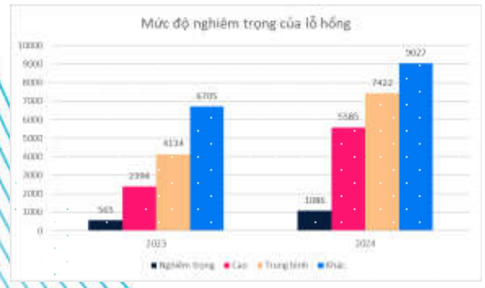
- Bối cảnh ATTT tại Việt Nam
- Thách thức với Chính quyền số và với ngành Công Thương

1.1 BỐI CẢNH ATTT TẠI VIỆT NAM 6T ĐẦU NĂM 2024

64%

▼

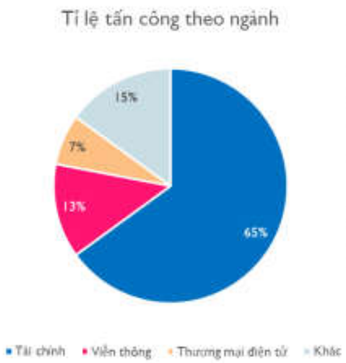
Số lượng lỗ hổng mới



1,6

▼

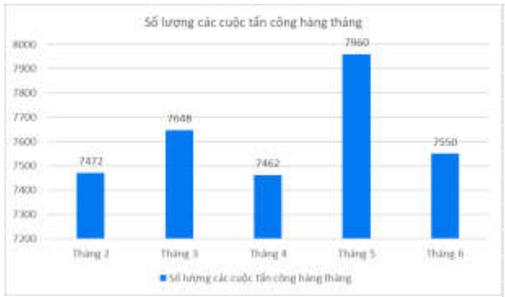
Số lượng tên miền giả mạo



60%

▼

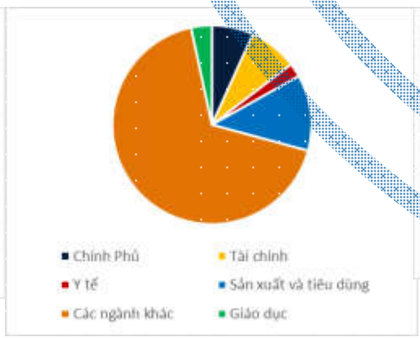
Số lượng các cuộc tấn công mạng



26%

▼

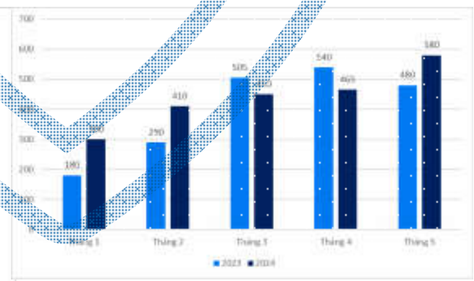
Số lượng tài khoản lộ lọt



1,3

▼

Số lượng cuộc tấn công ransomware



1.2 CÁC VỤ TẤN CÔNG RANSOMWARE TRONG NƯỚC

03/2024

Đơn vị **TOP 3 chứng khoán** trong nước

03/2024

Đơn vị **năng lượng quy mô lớn** tại Việt Nam

03/2024

Nhà mạng **viễn thông** ảo không hạ tầng TOP thị trường

04/2024

Các cổng thông tin **khối chính quyền**

Threat Intelligence Service

05/2024

TCT CP Bia rượu nước giải khát **KV miền Bắc**

Managed Security Service

06/2024

Tổng Công ty ngành **Bưu điện**

1.3 HÀNH LANG PHÁP LÝ

- Luật An toàn thông tin mạng **96/2015/QH13**
- Nghị định **85/2016/NĐ-CP**
- Luật an ninh mạng **24/2018/QH14**

→ Cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an toàn thông tin

- Chỉ thị **14/CT-TTg năm 2019**

→ Các bộ, cơ quan ngang bộ đảm bảo tỷ lệ kinh phí cho các SPDV ATTT mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng CNTT hàng năm

- Văn bản **1552/BTTTT-CATTT**

→ Triển khai bảo đảm ATTT theo mô hình “4 lớp”: (1) “Lớp 1” Lực lượng tại chỗ; (2) “Lớp 2” Tổ chúc hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp; (3) “Lớp 3” Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; (4) “Lớp 4” Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia

- Văn bản **708/BTTTT-CATTT**

→ Hướng dẫn các tiêu chi triển khai kỹ thuật đáp ứng kết nối với hệ thống CSDLQG về Dân Cư

1.3 THÁCH THỨC TRONG CHUYỂN ĐỔI SỐ CHÍNH QUYỀN

Hệ thống lớn và phức tạp

Hệ thống CNTT của các CQNN nước rất lớn và phức tạp, có sự kết nối liên thông giữa các đơn vị, có bối cảnh lịch sử triển khai khác nhau, do đó rất khó kiểm soát đảm bảo 100% an toàn bảo mật

Hiểm họa Ransomware toàn cầu

Vấn đề Ransomware đang trở nên nghiêm trọng trong những năm gần đây, vấn đề đảm bảo an toàn dữ liệu, đảm bảo dữ liệu có khả năng khôi phục khi có thảm hoạ trở nên cực kỳ quan trọng.

Khó khăn trong kiểm soát dữ liệu

Dữ liệu lưu trữ trên nhiều hệ thống, khó kiểm soát và phân loại, khó xác định dữ liệu nào quan trọng, mức độ quan trọng của từng loại dữ liệu

Quản lý hạ tầng

Hầu hết các CQNN đã quan tâm đến việc backup dữ liệu, đã triển khai các giải pháp Backup dữ liệu tại local site ở các phạm vi khác nhau (Backup 100% dữ liệu, hoặc chỉ Backup các dữ liệu quan trọng).

1.3 THÁCH THỨC VỚI NGÀNH CÔNG THƯƠNG

Dữ liệu lớn

- QĐ 3411/QĐ-BCT quy định danh mục 40 CSDL cho từng ngành nghề. Lượng dữ liệu này là cực kỳ lớn, liên thông giữa địa phương và trung ương nên việc quản lý, sao lưu, đảm bảo ATTT là cực kỳ thách thức

Kết nối nhiều Doanh nghiệp, ngành nghề

- Cơ sở dữ liệu Công thương mở cho các cá nhân, doanh nghiệp, tổ chức khai thác, sử dụng, nên sẽ là mục tiêu cho các cuộc tấn công mạng.

Liên thông đa ngành

- Dữ liệu liên thông giữa các ngành: GTVT, xây dựng, tài nguyên môi trường

02

CÂU CHUYỆN KHÁCH HÀNG

1.1 CÂU CHUYỆN KHÔI PHỤC SAU SỰ CỐ RANSOMWARE

1. GIAI ĐOẠN TRƯỚC SỰ CỐ

- Tháng 4/2024, VNPT khảo sát, tư vấn cho doanh nghiệp các phương án triển khai ATTT, sao lưu dữ liệu. Tuy nhiên do hệ thống lớn và phức tạp, các giải pháp ATTT chưa được triển khai đầy đủ. Doanh nghiệp mới chỉ kịp sao lưu các dữ liệu quan trọng lên VNPT Cloud.
- Sau khi khách hàng sao lưu dữ liệu lên VNPT Cloud, các dữ liệu này được bật cơ chế chống sửa/xoá để đảm bảo an toàn.

TRÊN **60**

kỹ sư CNTT và chuyên gia an toàn bảo mật sẵn sàng hỗ trợ **24/7 trong hơn 03 tuần**

TRÊN **50 TB**

Dữ liệu được **khôi phục** từ bản Backup

2. PHẢN ỨNG VỚI SỰ CỐ

- **Đầu tháng 6/2024, toàn bộ hệ thống dịch vụ khách hàng bị mã hóa bởi Ransomware, hoạt động SXKD bị tê liệt.**
- VNPT kích hoạt kịch bản phản ứng nhanh, huy động nguồn lực chuyên gia, hạ tầng, công nghệ để khôi phục dịch vụ cho khách hàng.
- Thực hiện song song các kịch bản: cô lập – điều tra, khôi phục hệ thống lên Cloud từ bản Backup, rà quét ATTT, tích hợp các giải pháp ATTT

EPS **5000**

Hệ thống **Giám sát ATTT của VNPT** dự kiến tích hợp cho KH này.

3. KHÔI PHỤC DỊCH VỤ

- Sau 4 ngày: các dịch vụ quan trọng nhất được khôi phục trên VNPT Cloud
- Sau 14 ngày: hầu hết các dịch vụ phục vụ SXKD của KH được khôi phục.

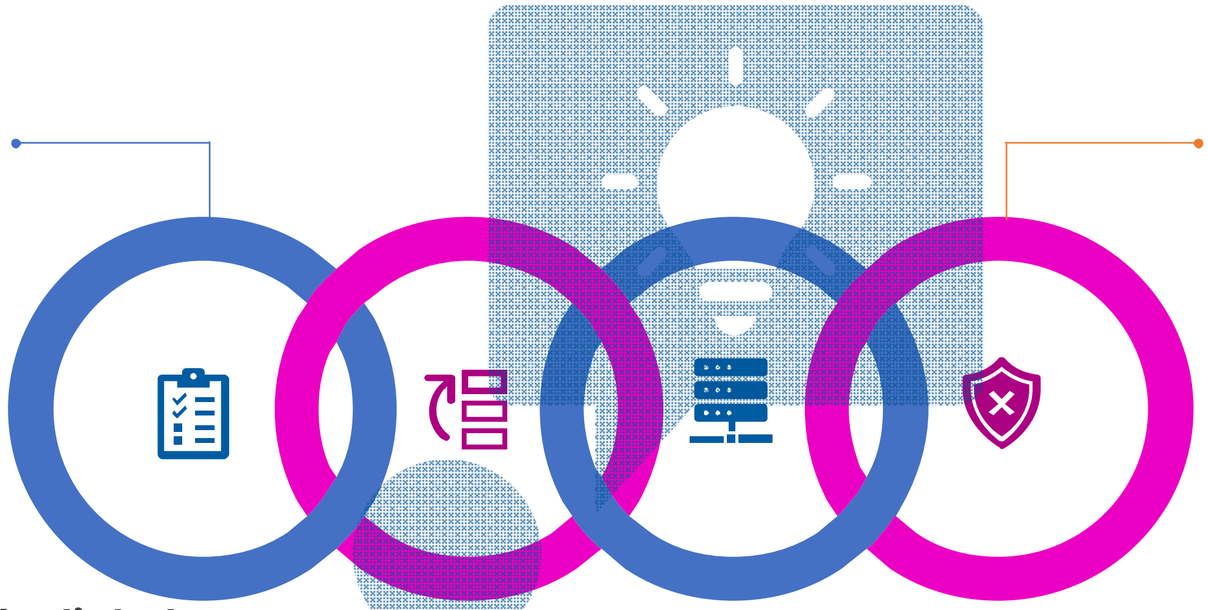
1.2 TỔ CHỨC KHÔI PHỤC

1. Điều phối, chịu trách nhiệm quyết định việc phối hợp và Go live
2. Rà soát an toàn, an ninh mạng cho các hệ thống đang cô lập
3. Khôi phục lại các hệ thống chính bị ảnh hưởng bởi mã độc tống tiền
4. Rà soát, đánh giá an toàn, an ninh mạng cho các hệ thống được dựng mới
5. Điều tra, phân tích sự cố

1.3 BÀI HỌC KINH NGHIỆM

Chưa có **kịch bản** ứng cứu sự cố

Chưa triển khai đầy đủ các **biện pháp** ATTT



Chưa xác định được **mức độ ưu tiên** các dịch vụ

Chưa **phân tách** hạ tầng Production và Backup

03

CHIẾN LƯỢC ĐẢM BẢO ATTT TRONG CHUYỂN ĐỔI SỐ

- Đảm bảo ATTT trong CĐS ngành Công Thương
- Đảm bảo ATTT trong CĐS chính quyền Tỉnh/Thành phố
- Chiến lược dữ liệu

3.1 CHIẾN LƯỢC ĐẢM BẢO ATTT CHÍNH QUYỀN ĐIỆN TỬ

1. Xác định tiêu chuẩn ATTT phù hợp: ATTT theo CĐ 3/4/5

2. Thiết kế ATTT cùng với thiết kế hạ tầng, đặc biệt với CSDL ngành Công thương

3. Xây dựng quy trình vận hành ATTT

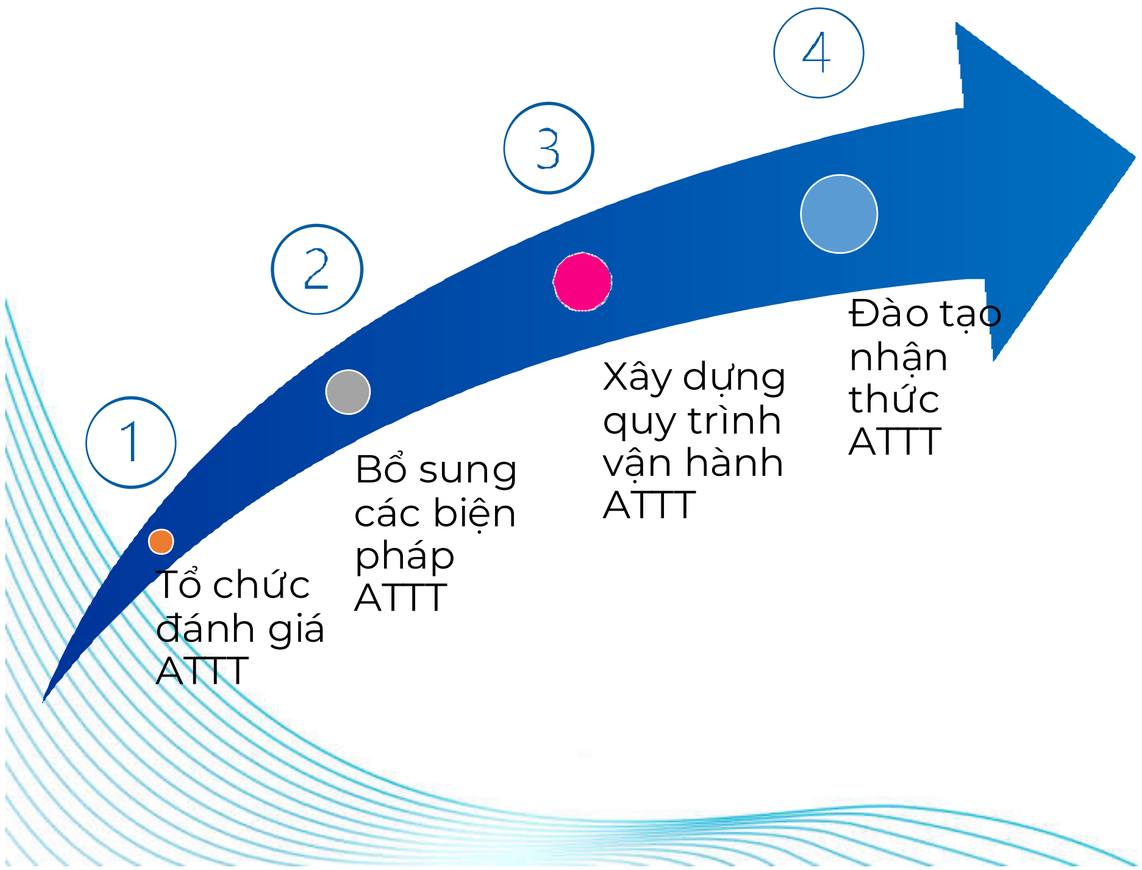
4. Xây dựng chiến lược dữ liệu

5. Tổ chức đào tạo nhận thức ATTT

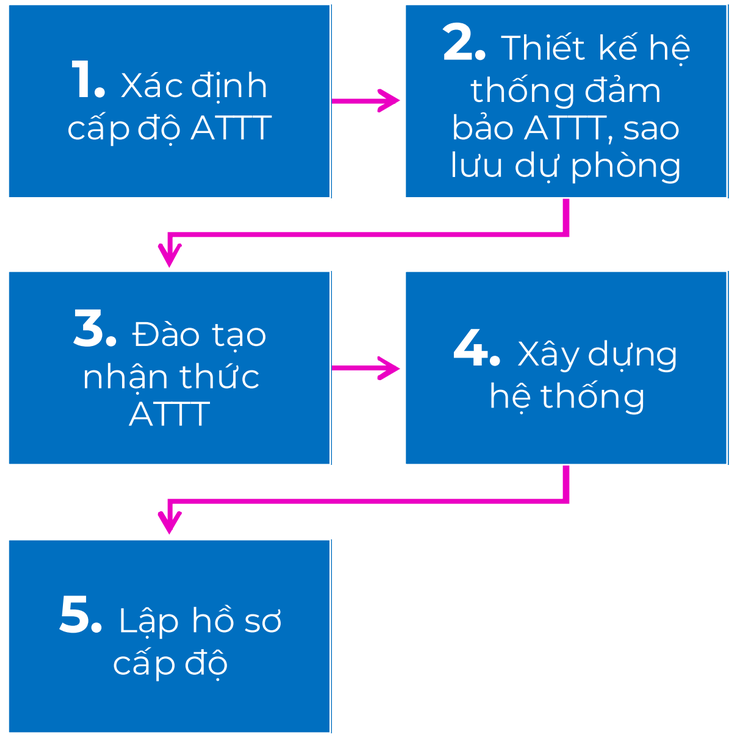
6. Diễn tập ATTT, diễn tập khôi phục hệ thống

3.2 CHIẾN LƯỢC TRONG XÂY DỰNG CSDL NGÀNH

Các Cơ quan đã có sẵn CSDL



Các Cơ quan đang xây dựng CSDL



3.3 CHIẾN LƯỢC BẢO VỆ DỮ LIỆU

01 PHÂN LOẠI, GẮN NHÃN DỮ LIỆU

02 XÁC ĐỊNH MỨC ĐỘ QUAN TRỌNG

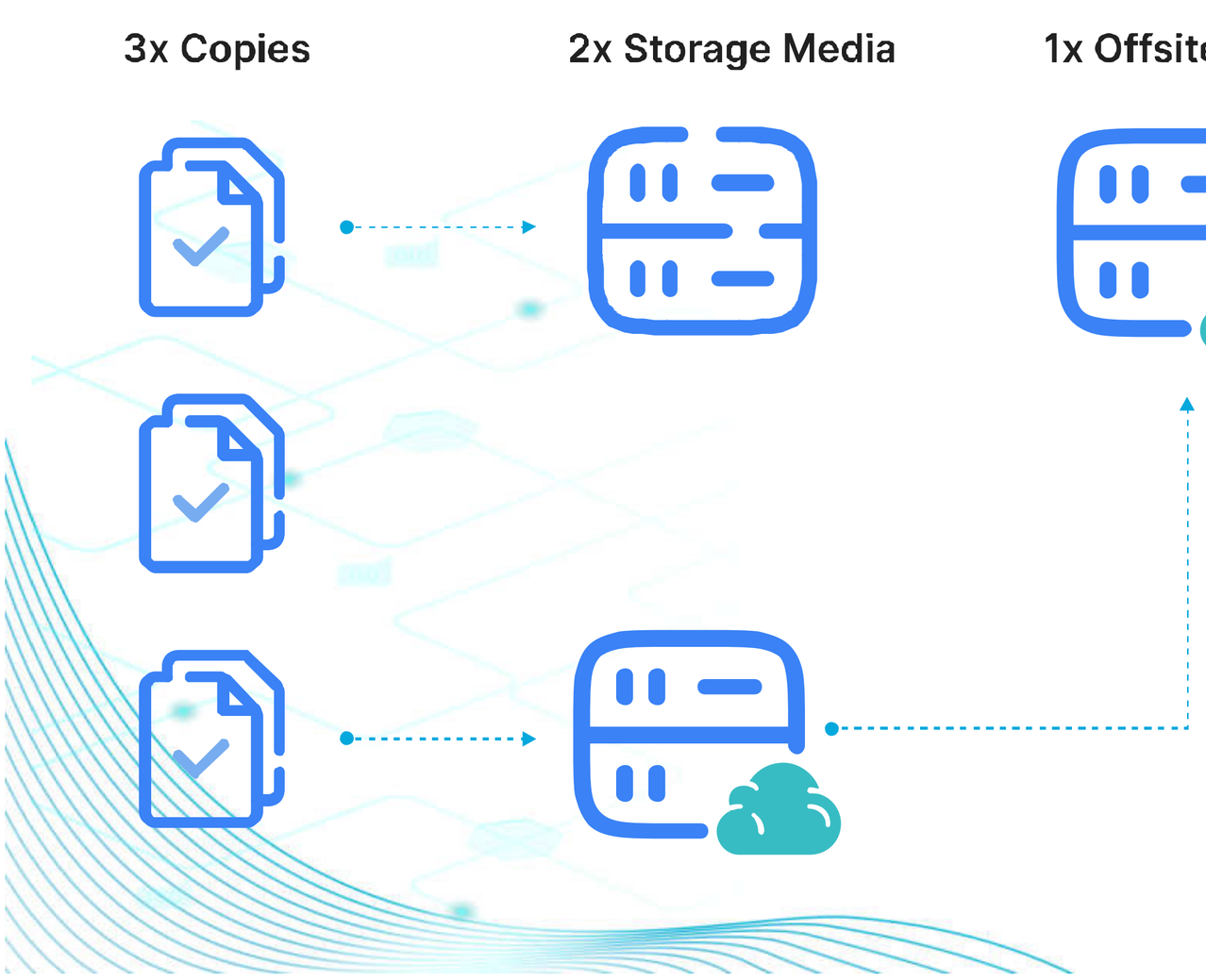
03 XÁC ĐỊNH QUYỀN TRUY CẬP DỮ LIỆU

04 XÁC ĐỊNH HÌNH THỨC SAO LƯU DỮ LIỆU

05 XÁC ĐỊNH TẦN SUẤT SAO LƯU DỮ LIỆU

06 XÂY DỰNG QUY TRÌNH XỬ LÝ/ SAO LƯU/KHÔI PHỤC DỮ LIỆU

3.4 CHIẾN LƯỢC SAO LƯU DỮ LIỆU 3-2-1-1-0

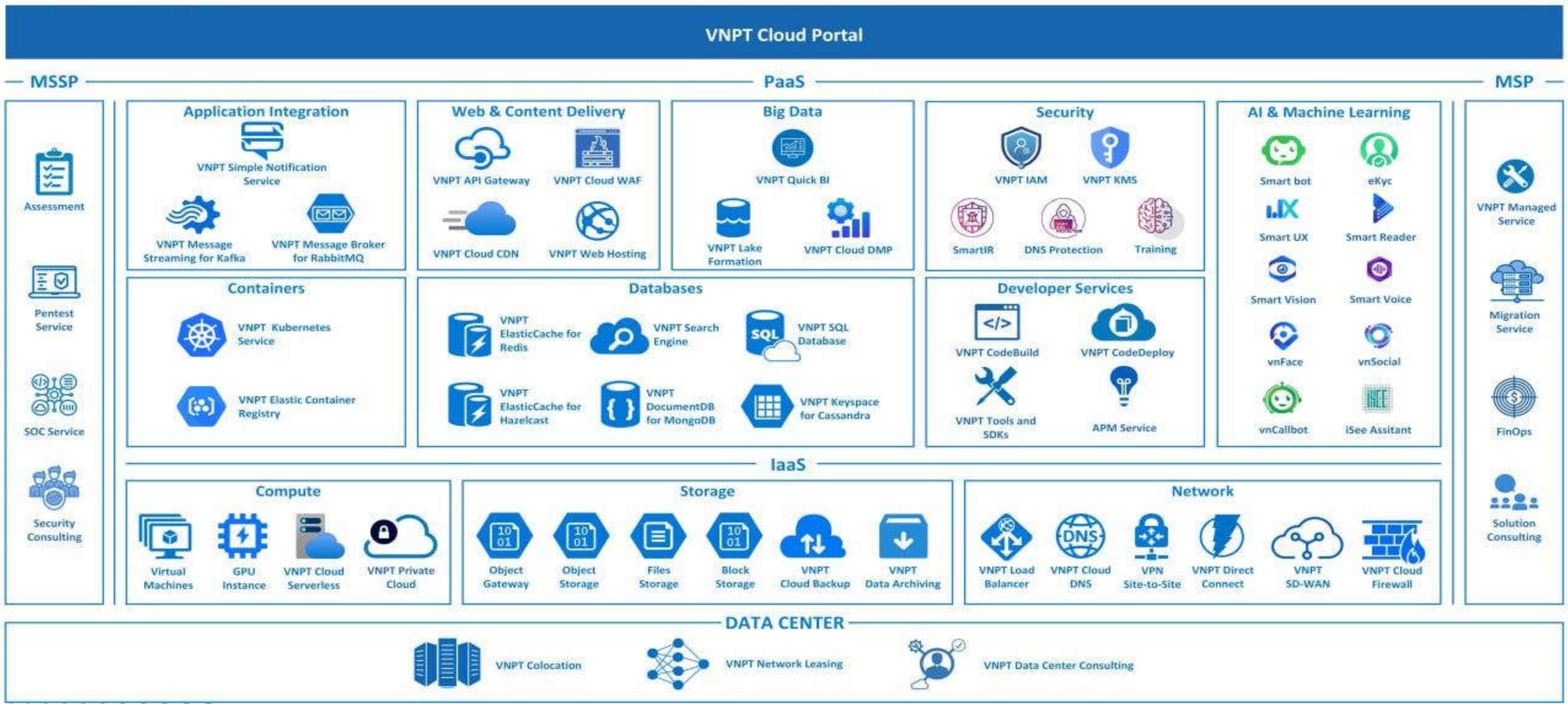


Chiến lược sao lưu **3-2-1** được quy định trong văn bản 2517/BTTTT-CATTT ngày 27/06/2024

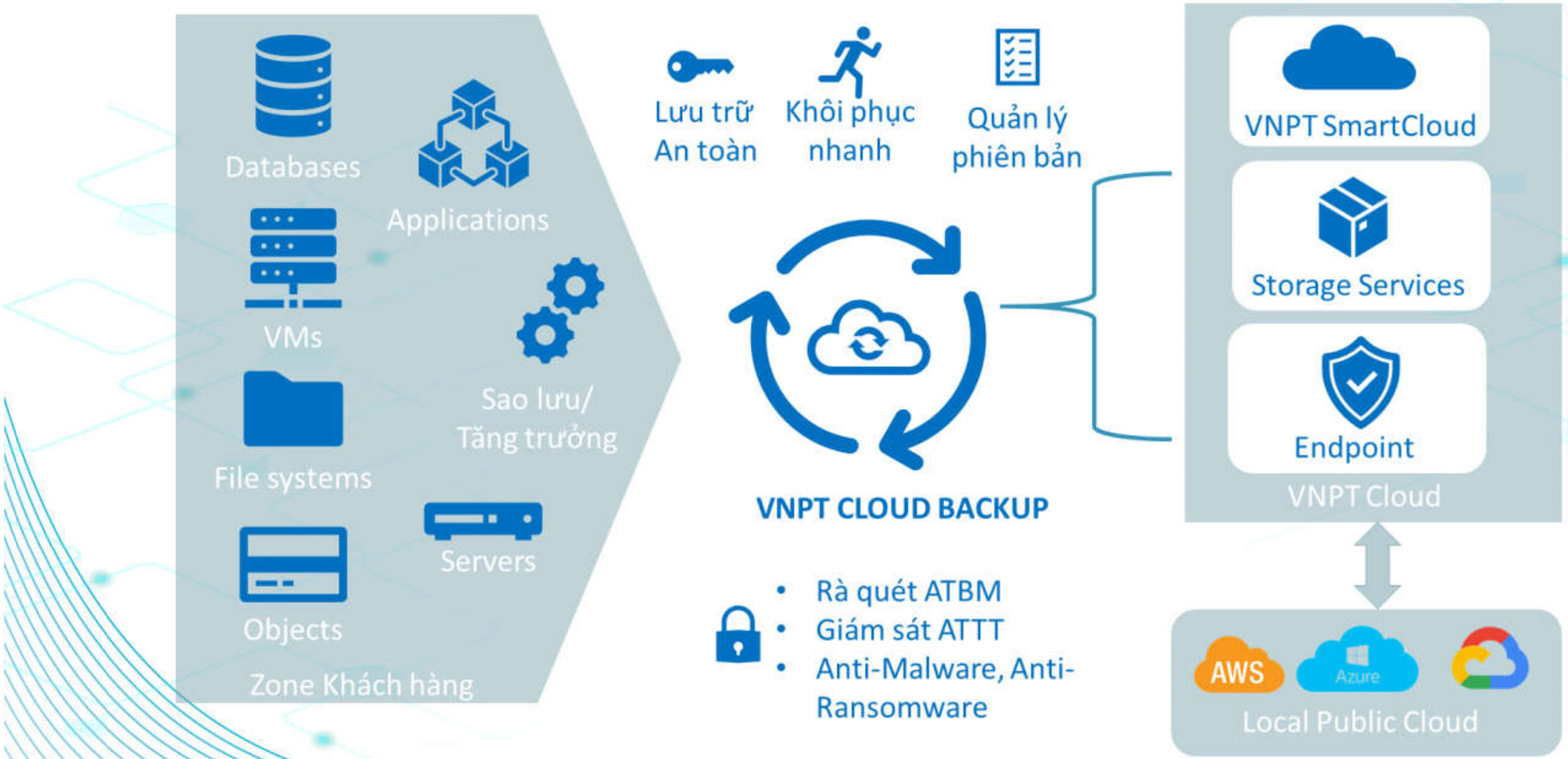
04

NĂNG LỰC, GIẢI PHÁP VỀ CLOUD, ATTT CỦA VNPT

4.1 HỆ SINH THÁI CHUYỂN ĐỔI SỐ CLOUD - ATTT



4.2 GIẢI PHÁP BẢO VỆ DỮ LIỆU



4.3 NĂNG LỰC CLOUD - ATTT

Năng lực về An toàn thông tin

- **Top 5** công ty an toàn thông tin tại Việt Nam. Hệ thống giám sát an ninh mạng lớn nhất Đông Nam Á
- Triển khai các dự án **an toàn thông tin cấp độ 3/4** cho Chính phủ, Bộ ngành
- Đội ngũ chuyên gia và kỹ sư đạt các **chứng chỉ QT uy tín**: CISSP, CEH, SEC+, OSWE, OSCP, CHFI, CISA, SOC Analyst và chứng chỉ ISO 27001:2013
- Đầy đủ các dịch vụ/giải pháp như Giám sát an toàn thông tin, Đánh giá an toàn thông tin, Giải pháp phát hiện và ứng cứu sự cố điểm cuối, kiểm soát kết nối độc hại

Đảm bảo an toàn, an ninh mạng cho hệ thống quan trọng

Năng lực hạ tầng lưu trữ, sao lưu

VNPTCloud

- Hạ tầng VNPT Cloud với hơn **1.000 máy chủ, 10PB lưu trữ**
- Triển khai trên **4 IDC** tiêu chuẩn Tier 3 tại Việt Nam
- Hệ sinh thái **40+ dịch vụ**, đa dạng các dịch vụ sao lưu dữ liệu, và các dịch vụ về ATTT
- Sẵn sàng triển khai các hệ thống yêu cầu Cấp độ 3/4, đáp ứng **VB 1552/708**
- Đội ngũ chuyên gia tư vấn, triển khai, quản trị vận hành.

Đảm bảo năng lực triển khai, vận hành các dự án CNTT quy mô toàn quốc

VNPT

TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG VIỆT NAM

TRÂN TRỌNG CẢM ƠN!