

**BÁO CÁO TÌNH HÌNH
AN TOÀN THÔNG TIN VIỆT NAM
6 THÁNG ĐẦU NĂM 2021**

MỤC LỤC

CẬP NHẬT TÌNH HÌNH AN TOÀN THÔNG TIN TRONG NƯỚC 6 THÁNG ĐẦU NĂM 2021	3
THỊ TRƯỜNG AN TOÀN THÔNG TIN TẠI VIỆT NAM NĂM 2021	7
YẾU TỐ BÊN NGOÀI TÁC ĐỘNG TỚI THỊ TRƯỜNG ATTT NĂM 2021.....	2
XU HƯỚNG AN TOÀN THÔNG TIN TẠI VIỆT NAM	17

CẬP NHẬT TÌNH HÌNH AN TOÀN THÔNG TIN TRONG NƯỚC 6 THÁNG ĐẦU NĂM 2021

Trong nửa đầu năm 2021, VCS-Threat Intelligence ghi nhận và phân tích rất nhiều cuộc tấn công lớn của các nhóm APT, cụ thể như sau:

- **Mức cao:**
 - Tháng 1/2021 - Cảnh báo chiến dịch tấn công của nhóm APT nhắm vào các nhà nghiên cứu bảo mật, sử dụng lỗ hổng 0-day khai thác RCE vào Google Chrome dựa vào Visual Studio Project.
 - Tháng 2/2021
 - Cảnh báo về chiến dịch tấn công người dùng lợi dụng một số bản cập nhật từ NoxPlayer. Trong chiến dịch, các hạ tầng của BigNox đã bị lợi dụng để phát tán mã độc.
 - Cảnh báo về hoạt động mới của nhóm APT32 được ghi nhận trên không gian mạng. Trong chiến dịch, nhóm APT32 sử dụng mã độc lợi dụng định dạng ActiveMime để tải về Cobalt Strike để tấn công người dùng Việt Nam.
 - Tháng 3/2021 - Cảnh báo về mẫu mã độc KerrDown Malware của nhóm APT32 nhắm vào người dùng Việt Nam.
 - Tháng 4/2021 - Cảnh báo hoạt động của nhóm APT Trung Quốc tấn công vào tổ chức ở Việt Nam. Chiến dịch diễn ra từ tháng 6/2020 đến tháng 01/2021 nhằm vào các tổ chức chính phủ, quân đội ở Việt Nam.
 - Tháng 5/2021
 - Nhóm APT 1937CN đã thực hiện tấn công có chủ đích vào Việt Nam lợi dụng các văn bản liên quan đến chính trị tại Việt Nam.
 - Chiến dịch tấn công lớn của một nhóm APT chưa xác định đã nhắm vào Việt Nam. Theo ghi nhận của VCS-Threat Intelligence, đã có nhiều trường hợp bị khai thác thành công.
 - Ghi nhận hàng chục biến thể mã độc của APT Trung Quốc đang ngày càng cải tiến so với các mẫu trước đây. Đây là loại mã độc có lịch sử tấn công mạng nhắm vào các tổ chức, cá nhân tại Việt Nam trong chiến dịch Supply Chain cuối năm 2020 và phần mềm giả lập NoxPlayer đầu năm 2021.
- **Mức trung bình:**
 - Cảnh báo các hoạt động mới của nhóm APT Trung Quốc tấn công trực tiếp vào Nga. Lịch sử tấn công có nhiều nét tương đồng với các chiến dịch nhắm vào Việt Nam trong quá khứ.
 - Cảnh báo mã độc Poison Ivy của APT Trung Quốc tấn công vào nhiều hạ tầng trên thế giới. Mã độc được sử dụng có nhiều nét tương đồng với chuỗi tấn công Supply Chain nhắm vào người dùng NoxPlayer đầu năm 2021.

Về lộ lọt thông tin, VCS – Threat Intelligence ghi nhận một số nguy cơ xảy ra trong nửa đầu 2021 như sau:

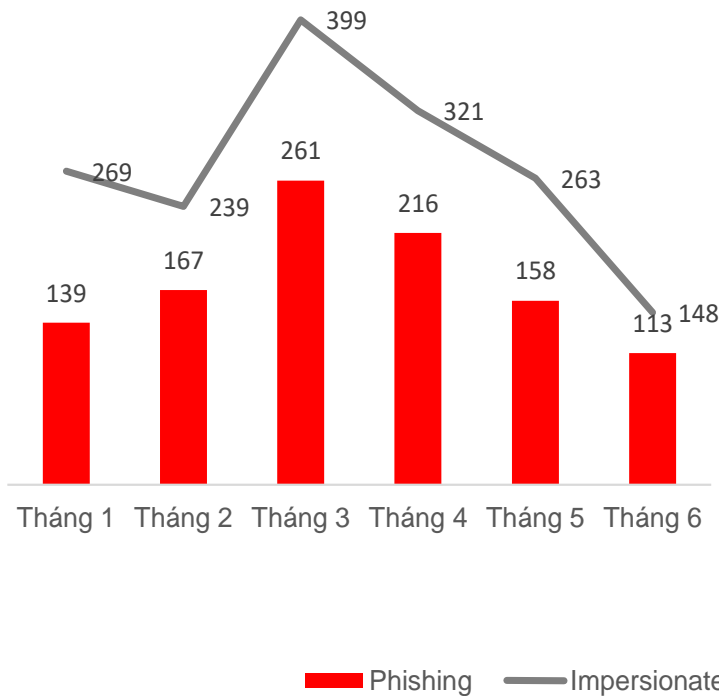
- Mức nghiêm trọng:
 - Nguy cơ dữ liệu bị lộ ra chứa hơn 77 triệu thông tin khách hàng đang được rao bán trên không gian mạng của những người dùng đã từng đăng ký hoặc sử dụng dịch vụ của NitroPDF.
 - Tập dữ liệu chứa hơn 1 triệu thông tin tài khoản của nhiều trang web xuất hiện trên Không gian mạng.
 - Rò rỉ 17GB dữ liệu KYC của người dùng tại Việt Nam, hàng nghìn chứng minh thư nhân dân bị rao bán trên không gian mạng.
- Mức trung bình:
 - Nhiều thông tin cá nhân của khách hàng xuất hiện trong nhiều tập dữ liệu dạng Combolist.
 - Trên diễn đàn RaidForums, dữ liệu liên quan tới Việt Nam được rao bán rất rầm rộ với các tiêu đề như :
 - 8.38 triệu bản ghi về dữ liệu dân cư và 2.8 triệu về doanh nghiệp Việt Nam.
 - Các văn bản tuyệt mật của Bộ Công an và Bộ Quốc phòng Việt Nam.
 - Dữ liệu 2 triệu người dùng từ các công ty bán lẻ điện máy.
 - Tập dữ liệu 50 nghìn người dùng từ sàn kết nối tài chính TIMA.

Nhìn chung, nửa đầu năm 2021 ghi nhận các vụ lộ lọt thông tin dữ liệu lớn khách hàng của các doanh nghiệp lớn Việt Nam (ngân hàng, tài chính, bán lẻ). Nguyên nhân được nhận định xuất phát từ:

- Việc khách hàng sử dụng email nội bộ để đăng ký cho các dịch vụ từ bên thứ ba không may bị rò rỉ thông tin.
- Máy tính cá nhân hoặc máy tính nội bộ bị nhiễm mã độc đánh cắp thông tin cá nhân.

Phishing/Impersonate (Lừa đảo, sử dụng thương hiệu của khách hàng)

Trong nửa đầu năm 2021, các hoạt động lừa đảo, lạm dụng thương hiệu diễn ra mạnh mẽ. Các cuộc tấn công lừa đảo gia tăng ở cả tần suất lẫn sự phức tạp, đặt ra mối đe dọa đáng kể với tất cả các tổ chức, đặc biệt là hình thức tấn công lừa đảo có chủ đích, nhằm vào các tổ chức tài chính, ngân hàng, các cổng thanh toán điện tử, ví điện tử. **Theo thống kê trên hệ thống của VCS - Threat Intelligence, 6 tháng đầu năm 2021, ghi nhận gần 3,000 domain lừa đảo, lạm dụng thương hiệu, gấp 3 lần so với cùng kỳ năm ngoái.**



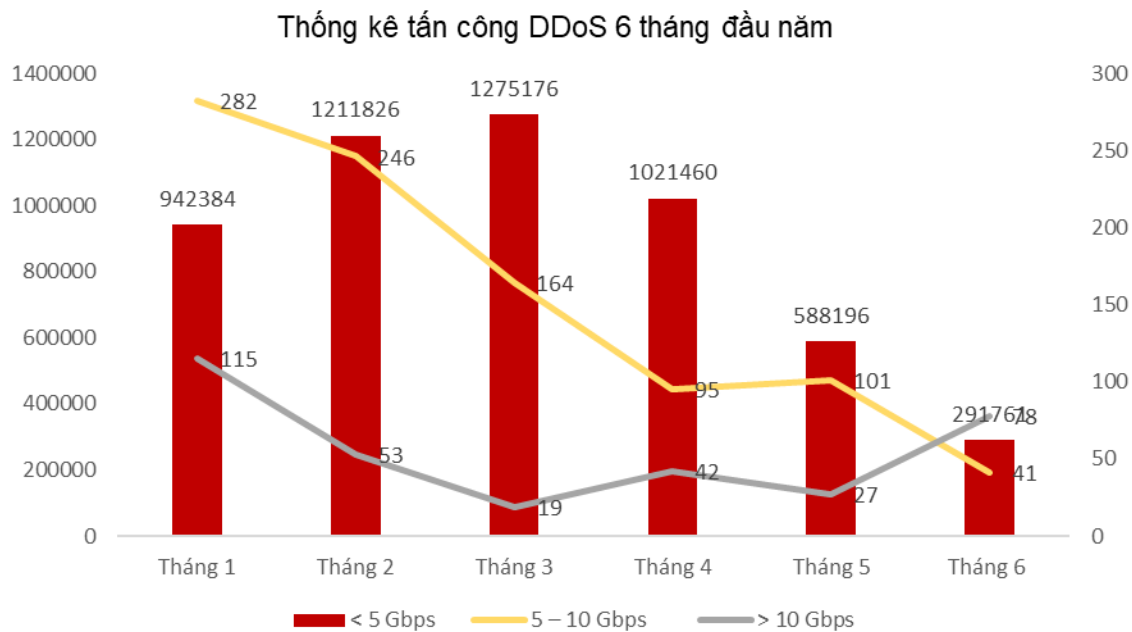
Báo cáo số lượng tấn công phishing, impersonate trong 6 tháng đầu năm

Các cuộc tấn công lừa đảo được chia thành 2 hình thức chính:

- Thông qua các trang mạng xã hội: Đối tượng giả mạo người mua các sản phẩm trên các group, trang bán hàng, đề nghị nạn nhân thực hiện giao dịch chuyển tiền online, lừa nạn nhân truy cập vào các đường link lừa đảo, hoặc lợi dụng các chương trình tri ân, trúng thưởng quà tặng để yêu cầu nạn nhân cung cấp thông tin cá nhân.
- Thông qua giả mạo SMS Brandname: Đây là hình thức đang phổ biến hiện nay, sử dụng tin nhắn định danh (SMS Brandname) giả để đánh lừa người dùng, tạo niềm tin đây là tin nhắn từ hệ thống thật, dụ họ đăng nhập vào website giả mạo nhằm đánh cắp thông tin tài khoản ngân hàng.

Tấn công DDoS tại Việt Nam. Thống kê số lượng tấn công theo các lưu lượng tấn công trong 6 tháng đầu năm 2021

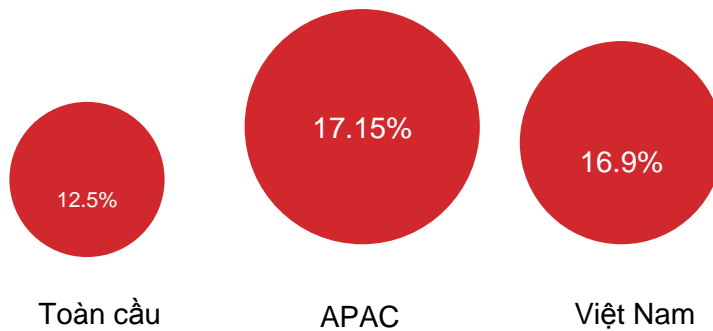
Lưu lượng tấn công	Số tấn công
0 - 1Gbps	5,969,306
1 Gbps - 2 Gbps	35,542
2 Gbps - 3 Gbps	5,090
3 Gbps - 4 Gbps	1,623
4 Gbps - 5 Gbps	854
5 Gbps - 6 Gbps	845
6 Gbps - 7 Gbps	185
7 Gbps - 8 Gbps	146
8 Gbps - 9 Gbps	117
9 Gbps - 10 Gbps	85
> 10 Gbps	581



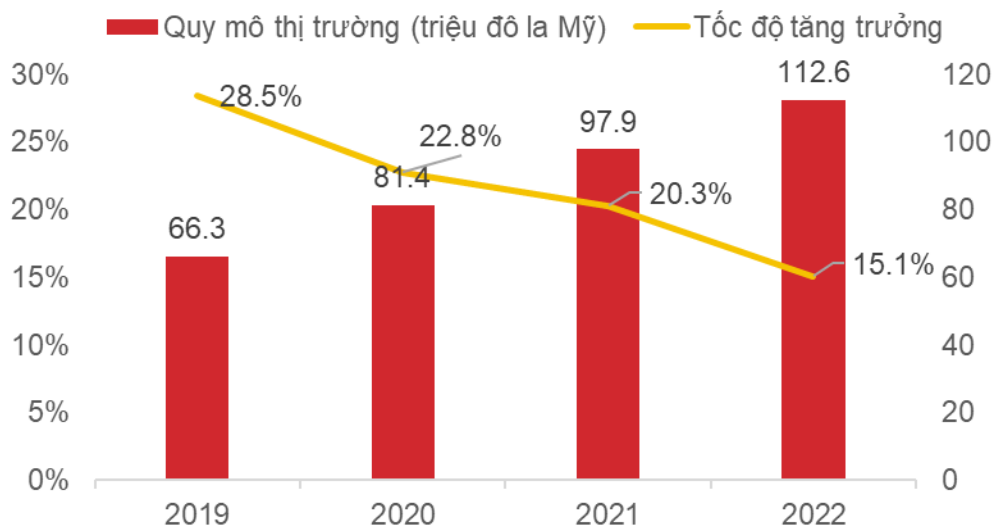
THỊ TRƯỜNG AN TOÀN THÔNG TIN TẠI VIỆT NAM NĂM 2021

Thị trường an toàn thông tin (ATTT) toàn cầu đạt 162.5 tỉ đô la Mỹ vào năm 2020 với tốc độ tăng trưởng hàng năm kép (CAGR 2020 - 2025) khoảng 12.5%, dự kiến đạt 418.2 tỉ đô la Mỹ vào năm 2028. Trong đó, khu vực Châu Á Thái Bình Dương (APAC) dự kiến đạt tốc độ CAGR từ 16 – 18.3% từ năm 2020 – 2025 (Mordor Intelligence, 2021 và Gartner, 2021).

Thị trường Việt Nam với tốc độ tăng trưởng CAGR khoảng 16.9%, có quy mô khoảng 61.3 triệu đô (tương đương khoảng 1409 tỉ đồng Việt Nam) vào năm 2019 và đạt 81.4 triệu đô la Mỹ vào năm 2020 (Ken Research, 2021). Trong năm 2021, quy mô thị trường ATTT Việt Nam dự kiến đạt 97.9 triệu đô la Mỹ, tương đương 2,252 tỉ đồng Việt Nam.



Tốc độ tăng trưởng kép (CAGR) hàng năm 2020 – 2025 (Ken Research, Mordor Intelligence, Gartner)



Quy mô và tốc độ tăng trưởng hàng năm

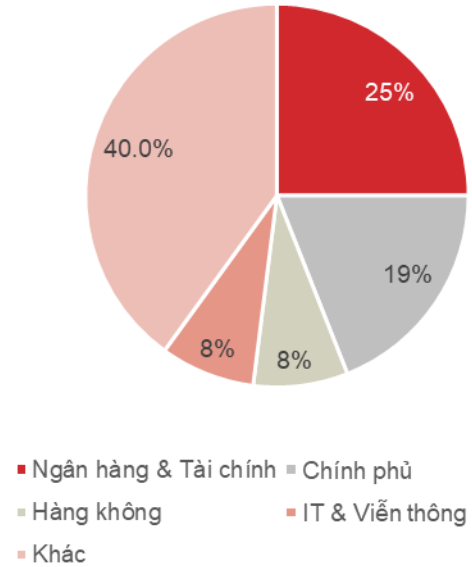
thị trường Việt Nam năm 2019 – 2022 (Ken Research, 2021)

Tỉ trọng theo nhóm khách hàng

Theo báo cáo của Ken Research, với mức độ trưởng thành ATTT cao, Tài chính và Ngân hàng chiếm phần lớn tỉ trọng nhu cầu về ATTT tại thị trường Việt Nam. Trong đó đặc biệt là nhóm Ngân hàng Thương mại cổ phần và các công ty chứng khoán có sự bùng nổ về lượng giao dịch trong năm 2020 và nửa đầu năm 2021.

Các chỉ định và thông tư của Chính phủ về bảo mật, ATTT góp phần gia tăng nhu cầu trong nhóm Chính phủ và nhà nước. Ngoài các đơn vị tỉnh, Ngân hàng, Kho bạc nhà nước, một số đơn vị liên quan tới Y tế và Sức khỏe bắt đầu chú trọng vào ATTT do tình hình diễn biến COVID-19 phức tạp và thông tin vắc-xin.

Quy mô thị trường theo ngành
(Ken Reserach, 2019)

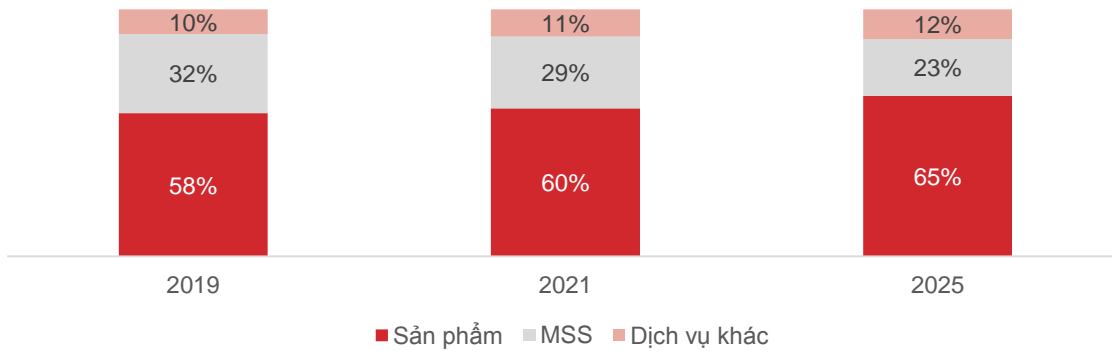


Tỷ trọng doanh thu của các giải pháp An toàn thông tin tại Việt Nam

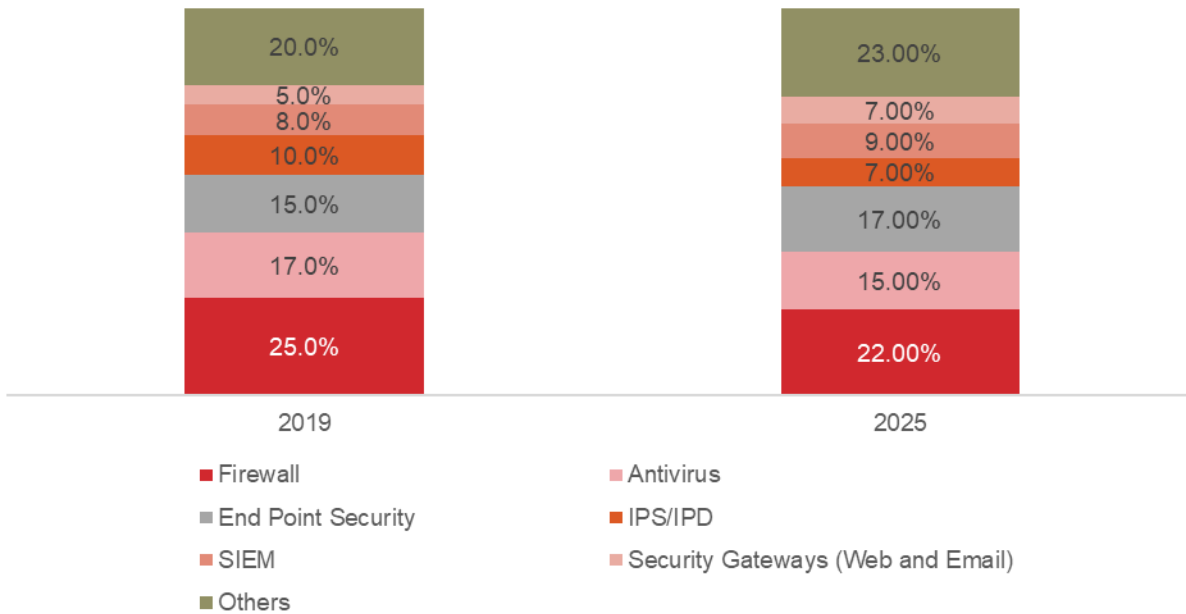
Sản phẩm và dịch vụ ATTT standalone chiếm tỷ trọng thị phần cao trên 50% và có xu hướng tăng từ năm 2019 – 2025. Dịch vụ MSS chiếm tỷ trọng trong khoảng từ 32% - 23% thị phần, có xu hướng giảm trong năm 2019 – 2025.

Theo loại hình sản phẩm, các dòng sản phẩm Firewall vẫn nắm giữ tỉ trọng cao nhất từ 25% năm 2019 tới 22% vào năm 2025. Antivirus và Endpoint security có sự thay đổi không đáng kể, khoảng 15-17%.

Tỷ trọng doanh thu theo các giải pháp ATTT Việt Nam 2019 - 2025
(Ken Research)



Tỷ trọng doanh thu theo loại hình sản phẩm ATTT tại Việt Nam, 2019 - 2025
(Ken Research)

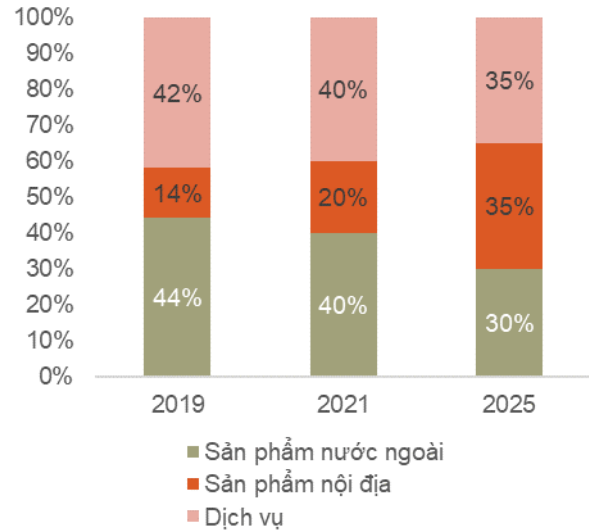


Theo báo cáo của Ken Research, thị trường ATTT tại Việt Nam có sự cạnh tranh gay gắt giữa các hãng nội địa và hãng nước ngoài.

Về sản phẩm, năm 2019 chiếm 75% sản phẩm nước ngoài, 25% sản phẩm nội địa. Năm 2025, dự kiến sản phẩm nước ngoài giảm còn 46%, sản phẩm trong nước tăng 54%.

Về dịch vụ, dịch vụ SOC, Pentest, Security Audit là các dịch vụ nổi bật được cung cấp nhiều bởi các công ty nội địa nhờ vào tính cạnh tranh con người, chuyên gia và đội ngũ xử lý sự cố nhanh chóng, kịp thời.

% sản phẩm & dịch vụ nội địa nước ngoài 2019 - 2025



Tuy nhiên với khoảng 20 hãng nước ngoài thông qua kênh phân phối tạo sức cạnh tranh lớn tại thị trường với các dòng sản phẩm: Firewalls, EDR, Security Web Gateway, Security Email Gateway, SIEM/ SOAR.

Với mô hình kinh doanh direct to customer và qua kênh phân phối, các doanh nghiệp ATTT Việt Nam dần mở rộng thị phần nhờ vào lợi thế cạnh tranh nội địa, hành lang pháp lý. Tuy nhiên, điều đó không phủ nhận sức cạnh tranh cao từ các hãng nước ngoài.

Năm 2025 dự đoán thị phần sản phẩm nội địa tăng 21%, đạt 35% ngang với dịch vụ ATTT. Sản phẩm nước ngoài dự đoán giảm thị phần từ 44% (2019) xuống 30% (2025).

Yếu tố thúc đẩy nhu cầu An toàn thông tin tại thị trường Việt Nam

Sự gia tăng các nguy cơ tấn công mạng là yếu tố quan trọng nhất dẫn đến sự gia tăng nhu cầu về ATTT tin tại Việt Nam. Các yếu tố khác như quy định, văn bản pháp luật về ATTT cũng góp phần không nhỏ vào nhu cầu ATTT.

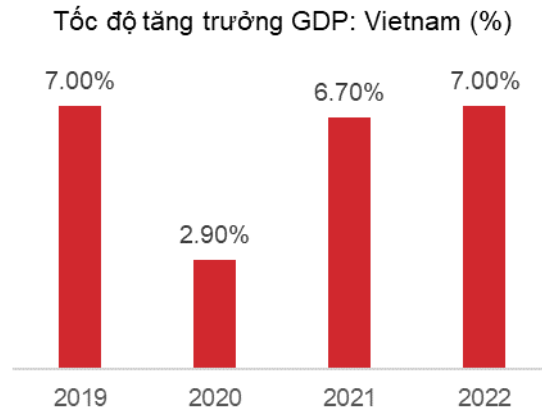
Gia tăng nhu cầu	Sự gia tăng nguy cơ tấn công mạng	<ul style="list-style-type: none"> - Năm 2021 ghi nhận sự gia tăng tấn công an ninh mạng vào các tổ chức tài chính, ngân hàng và chính phủ Việt Nam - Kịch bản tấn công và mức độ phức tạp của các vụ tấn công ngày càng gia tăng
	Quy định, văn bản pháp luật Việt Nam	<ul style="list-style-type: none"> - Thông tư số 09/2020/TT-NHNN quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng, ban hành ngày 21/10/2020 - Công văn 1552/BTTTT- CATT V/v Đôn đốc tổ chức triển khai đảm bảo ATTT theo mô hình “4 lớp” ban hành ngày 28/04/2020
	Sự thiếu hụt nhân sự ngành ATTT	<ul style="list-style-type: none"> - Nhân sự ATTT thiếu hụt, đặc biệt các chuyên gia có năng lực cao, đảm bảo quản trị an ninh mạng in-house của các tổ chức, doanh nghiệp - Công tác đào tạo, nâng cao năng lực nhân sự ATTT còn hạn chế
	Xu hướng công nghệ thông tin	<ul style="list-style-type: none"> - Sự gia tăng các giải pháp trên hạ tầng cloud tạo nên thách thức mới cho an ninh mạng - Xu hướng “work from home” của các doanh nghiệp, tổ chức tiềm ẩn nhiều nguy cơ tấn công mạng - Ứng dụng IoT và Machine Learning trong các giải pháp vận hành ATTT
Giá cả	Cạnh tranh giá cả	Thị trường cạnh tranh giữa các hãng nước ngoài và nội địa, trong đó các hãng nước ngoài với ưu thế thương hiệu, công nghệ và chứng chỉ. Hãng nội địa cạnh tranh về nhân sự trong nước và giá cả.
	Cơ chế giá linh hoạt theo nhu cầu	Chiến lược và cơ chế giá linh hoạt theo nhu cầu của khách hàng trong nước

YẾU TỐ BÊN NGOÀI TÁC ĐỘNG TỚI THỊ TRƯỜNG ATTT NĂM 2021

Tình hình kinh tế Việt Nam 2021

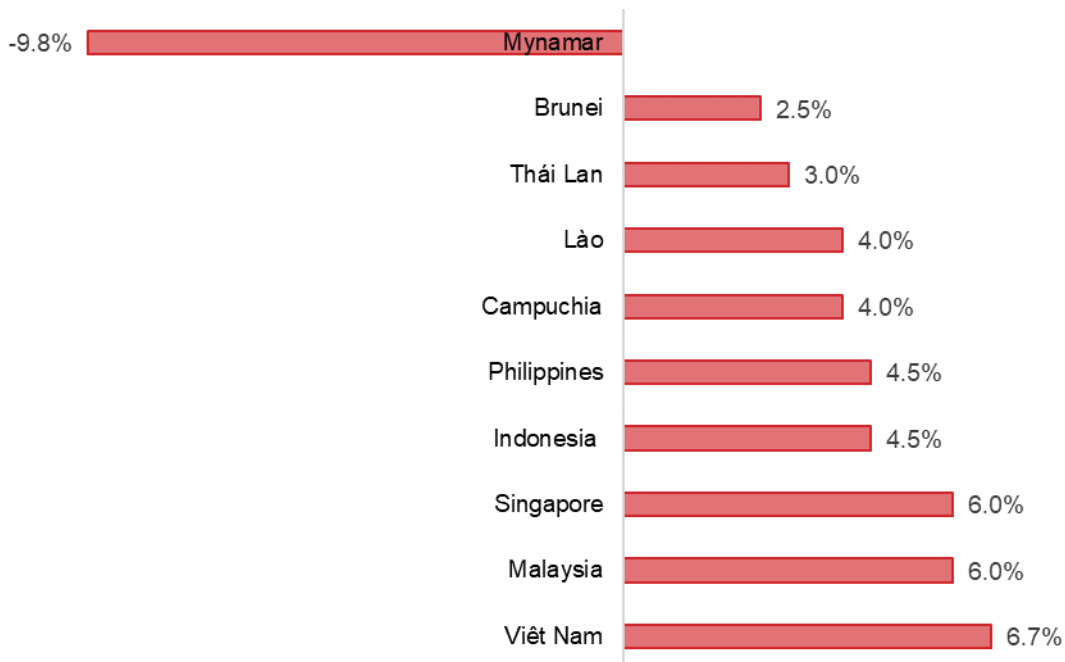
Theo báo cáo của Asia Development Bank 2021, tăng trưởng GDP của Việt Nam dự báo đạt 6,7% trong năm 2021 và 7% vào năm 2022. Tăng trưởng GDP đầu người dự báo đạt 5,4% trong năm 2021 và 5,6% năm 2022. Việt Nam được dự đoán là nước có tốc độ tăng trưởng GDP năm 2021 cao nhất trong khu vực Đông Nam Á. Nhìn chung, kinh tế Việt Nam có sự hồi phục khá nhanh so với các nước trong khu vực trong năm 2021.

Tuy nhiên các hoạt động đầu tư vào ATTT của các bộ, ban, ngành có thể chững lại vì ưu tiên nguồn kinh phí cho cứu trợ COVID-19 và hồi phục các ngành kinh tế.



Nguồn: Asia Development Bank, Asian Development Outlook 2021

Dự đoán tốc độ tăng trưởng GDP 2021



Tình hình chính trị, xã hội Việt Nam tính tới nửa đầu năm 2021

Trong 6 tháng đầu năm 2021 ghi nhận sự kiện chính trị lớn của năm - Bầu cử quốc hội khóa XV nhiệm kỳ 2021 – 2026. Tính đến 23/5/2021 cả nước có 99,57% cử tri đi bầu cử. Căn cứ vào biên bản tổng kết cuộc bầu cử trong cả nước, Hội đồng bầu cử quốc gia tiến hành công bố kết quả bầu cử và danh sách những người trúng cử đại biểu Quốc hội chậm nhất là ngày 12/6/2021 (hoặc 20 ngày sau ngày bầu cử). Bầu cử quốc hội là sự kiện quan trọng ảnh hưởng đến tình hình kế hoạch đầu tư chi phí của các tỉnh trong nửa đầu năm 2021 không có quá nhiều dự án mở thầu.

Tại Nghị quyết phiên họp Chính phủ thường kỳ tháng 5/2021, Chính phủ thống nhất với đề nghị của Bộ Tài chính tại văn bản số 103/TTr-BTC ngày 02/06/2021 về: Cắt giảm tối thiểu 50% kinh phí hội nghị, công tác trong và ngoài nước còn lại của các bộ, cơ quan trung ương, địa phương (Trừ các hoạt động quan trọng, cấp bách và phục vụ công tác phòng chống dịch của các Bộ: Bộ Quốc phòng, Bộ Công an, Bộ Y tế, kinh phí hoạt động ngoại giao quốc gia khác của Bộ Ngoại giao) và tiết kiệm thêm 10% chi thường xuyên còn lại của năm 2021 để bổ sung nguồn phòng, chống dịch COVID-19, tăng đầu tư phát triển và nhiệm vụ an ninh, quốc phòng cần thiết.

Báo cáo quốc hội cho phép thu hồi các khoản kinh phí thường xuyên đã giao cho các Bộ, cơ quan trung ương và địa phương nhưng đến ngày 30/6/2021 chưa phân bổ hoặc đã phân bổ nhưng chưa triển khai thực hiện (chưa phê duyệt dự đoán, chưa tổ chức đấu thầu) và các khoản phí thường xuyên chưa thực sự cần thiết để bổ sung nguồn dự phòng ngân sách trung ương và ngân sách địa phương chi cho công tác phòng, chống dịch COVID-19 và phục vụ chiến dịch vắc-xin.

Tình hình COVID-19 đến giữa năm 2021 vẫn vô cùng phức tạp, ảnh hưởng đến kế hoạch chi tiêu và đầu tư của các bộ, ban, ngành và các địa phương.

“Cắt giảm tối thiểu 50% kinh phí hội nghị, công tác trong và ngoài nước còn lại của các bộ, cơ quan trung ương, địa phương (Trừ các hoạt động quan trọng, cấp bách và phục vụ công tác phòng chống dịch của các Bộ: Bộ Quốc phòng, Bộ Công an, Bộ Y tế, kinh phí hoạt động ngoại giao quốc gia khác của Bộ Ngoại giao) và tiết kiệm thêm 10% chi thường xuyên còn lại của năm 2021 để bổ sung nguồn phòng, chống dịch COVID-19, tăng đầu tư phát triển và nhiệm vụ an ninh, quốc phòng cần thiết.”

Trích “Văn bản số 103/TTr-BTC ngày 02/6/2021 của Bộ tài chính”

Tình hình pháp luật Việt Nam tính tới nửa đầu năm 2021

Ngoài các thông tin luật pháp nổi bật trước năm 2020 liên quan tới ATTT tại Việt Nam như:

Cập nhật về luật pháp liên quan tới An toàn thông tin tại Việt Nam (2015 – 2021)

Số hiệu	Nội dung chính	Các điểm nổi bật
Chỉ thị 14/CT-TTg năm 2019	Về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam	<p>Các bộ, cơ quan ngang bộ bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ ATTT mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm</p> <p>Đối với công tác giám sát, ứng cứu sự cố ATTT mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý: Kết nối, chia sẻ thông tin với Trung tâm Giám sát không gian mạng quốc gia</p>
Quyết định 1017/QĐ-TTg năm 2018	Đề án giám sát ATTT mạng đối với hệ thống dịch vụ CNTT phục vụ chính phủ điện tử đến năm 2020, định hướng đến năm 2025	Khuyến khích các cơ quan nhà nước thuê dịch vụ kỹ thuật và nhân sự trong triển khai giám sát ATTT mạng cho hệ thống phục vụ Chính phủ điện tử.
Luật An ninh mạng 24/2018/QH14	Luật An ninh mạng	Luật quy định về hoạt động bảo vệ An ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.
Thông tư 31/2017/TT-BTTTT	Quy định hoạt động giám sát an toàn hệ thống thông tin	Doanh nghiệp dịch vụ ATTT mạng có trách nhiệm phối hợp với chủ quản hệ thống thông tin trong việc giám sát yêu cầu của Bộ Thông tin và Truyền thông (Bộ TT&TT), cung cấp các thông tin về hạ tầng kỹ thuật theo yêu cầu và phục vụ cho hoạt động giám sát của Bộ TT&TT.
Quyết định 05/2017/QĐ-TTg	Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia	Kinh phí thực hiện các hoạt động ứng cứu sự cố ATTT mạng được bố trí trong dự toán chi ngân sách nhà nước. Ngân sách trung ương đảm bảo cho hoạt động cơ quan điều phối quốc gia, hỗ trợ xây dựng, áp dụng chuẩn ISO 27xxx và các chuẩn quốc tế về ATTT mạng.

Năm 2020 và 2021, tình hình luật pháp có một số điểm nổi bật như **Công văn số 1552/BTTTT-CATT V/v Đôn đốc tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin theo mô hình “4 lớp”**.

Trong đó, đề nghị các bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, các ủy ban nhân dân tỉnh thành phố trực thuộc Trung ương hoàn thành việc triển khai bảo đảm ATTT cho hệ thống thông tin theo mô hình “4 lớp” trước ngày 30/09/2020.

Ngày 15/06/2021, Bộ Thông tin và Truyền thông đã ban hành **Công văn số 2085/BTTTT-CATT V/v khuyến khích sử dụng sản phẩm, giải pháp an toàn, an ninh mạng Make in Việt Nam**. Theo đó, Bộ Thông tin và Truyền thông đã thực hiện nghiên cứu, đánh giá và lựa chọn những sản phẩm an toàn, an ninh mạng tiêu biểu do doanh nghiệp Việt Nam sản xuất để khuyến nghị các cơ quan, tổ chức, doanh nghiệp nghiên cứu sử dụng theo nhu cầu thực tiễn của tổ chức, doanh nghiệp trong nước. Danh sách bao gồm:

1. *Sản phẩm an toàn cho thiết bị đầu cuối:*
 - Viettel Endpoint Detection & Response
 - Giải pháp phân tích hành vi bất thường (VCS – KIAN)
 - CMC Malware Detection and Defence
 - Phần mềm diệt vi-rút Bkav Endpoint AI
 - Cyradar – EDR
 - FPT.EagleEye MDR
2. *Sản phẩm an toàn lớp mạng*
 - RealTech UTM Firewall
 - Viettel Network Access Control
 - Viettel Anti-DDoS
 - Viettel Security Information & Event Management
 - Viettel Network Security Monitoring
 - FPT.EagleEye malBOT
 - Bkav – IPS Firewall
 - Giải pháp kiểm soát chính sách an ninh – Bkav Total NAC
 - CyRadar – SIEM
 - FPT.EagleEye mGuard
3. *Sản phẩm an toàn lớp ứng dụng*
 - Viettel Web Application Firewall/ Viettel Smart Web Protection
 - Viettel Email Security Gateway
 - Hệ thống phát hiện các mối đe dọa nâng cao (CyRadar – Advanced Threads Detection System)
 - RealTech WAF
 - RealTech Antispam mail
4. *Giải pháp an toàn, an ninh mạng khác*
 - Viettel Threat Intelligence
 - Viettel Security Orchestration Automation & Response
 - Nền tảng quản lý an toàn thông tin – VNPT MSS
 - VNCS Phần mềm rà soát hạ tầng mạng internet VNCS CyberScan

Một số cập nhật mới nhất về luật pháp liên quan tới ATTT năm 2021 nổi bật với thông tin: Ngân hàng nhà nước Việt Nam ban hành Thông tư số 09/2020/TT-NHNN có hiệu lực thi hành từ ngày 01/01/2021.

Thông tư 09/2020/TT-NHNN

Quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng

Thông tư này áp dụng đối với các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng dịch vụ trung gian thanh toán, công ty thông tin tín dụng, công ty cổ phần Thanh toán quốc gia Việt Nam, Công ty quản lý tài sản của tổ chức tín dụng Việt Nam, Nhà máy in tiền quốc gia, Bảo hiểm tiền gửi Việt Nam

Tổ chức rà soát quy chế ATTT tối thiểu mỗi năm một lần.

Quản lý sử dụng thiết bị di động: Các thiết bị di động khi kết nối hệ thống mạng nội bộ phải được đăng ký để kiểm soát. Với thiết bị di động là tài sản của tổ chức, kiểm soát các phần mềm cài đặt, sử dụng tính năng bảo vệ thông tin cá nhân, thông tin nội bộ, thông tin bí mật, thiết lập mã khóa bí mật, cài phần mềm chống mã độc và các lỗi bảo mật khác.

Hệ thống dịch vụ giao dịch trực tuyến phải được áp dụng các biện pháp để giám sát chặt chẽ và phát hiện, cảnh báo về:

- Giao dịch đáng ngờ dựa vào các tiêu chí tối thiểu gồm: thời gian giao dịch, địa điểm giao dịch (vị trí địa lý, địa chỉ IP mạng), tần suất giao dịch, số tiền giao dịch, số lần xác thực sai quy định;
- Hoạt động bất thường của hệ thống;
- Các cuộc tấn công từ chối dịch vụ (DoS - Denial of Service attack), tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service attack).

Tổ chức có trách nhiệm gửi báo cáo về Ngân hàng Nhà nước (Cục Công nghệ thông tin): Báo cáo sự cố ATTT trong vòng 24 giờ kể từ thời điểm sự cố được phát hiện và báo cáo hoàn thành khắc phục sự cố trong vòng 05 ngày làm việc sau khi hoàn thành khắc phục sự cố.

Nhìn chung, thông tư 09/2020/TT-NHNN của Ngân hàng nhà nước rất chi tiết về yêu cầu bảo mật ATTT trong ngân hàng và các tổ chức tín dụng, tài sản. Đặc biệt khuyến khích sử dụng các sản phẩm, dịch vụ có chứng chỉ quốc tế. Tuy nhiên điều này cũng gây ra sự cạnh tranh rất lớn giữa hãng nước ngoài với các hãng nội địa vì không có yêu cầu nào đòi hỏi sản phẩm Make in Việt Nam và các điểm nổi bật của sản phẩm (selling points) chỉ các hãng nội địa mới cung cấp được.

Ngân hàng, nhóm ngành dẫn đầu về An toàn thông tin tại Việt Nam

Nhóm ngân hàng được đánh giá có độ trưởng thành tương đối cao trong ATTT ở Việt Nam. Về tăng trưởng năm 2020, ngân hàng vẫn tăng 3%, dự báo tăng 15% vào năm 2021 (Báo cáo thị trường ngân hàng của SSI, 2020). Tăng trưởng tín dụng giảm vào năm 2020, kỳ vọng phục hồi vào năm 2021 (11-12%).

Nhóm ngân hàng năng động (ACB, MBB, TCB, VPB, VIB, TPB) nhóm có tốc độ tăng trưởng cao hơn về tín dụng, ghi nhận tăng trưởng khả quan, ít áp lực lãi suất đầu ra.

Nhóm ngân hàng lớn (AGR, VCB, BIDV, Viettin) áp lực giảm lãi suất đầu ra, chưa phục hồi hoàn toàn vào 2021. (Vietcombank Security Report, 2020).

Ngân sách dành cho ATTT của nhóm ngân hàng khoảng 10-15% tổng ngân sách công nghệ thông tin. Tình hình COVID-19 căng thẳng trong 6 tháng đầu năm 2021 đi kèm các vụ tấn công an ninh mạng vào hệ thống ngân hàng Việt Nam, thúc đẩy nhanh hơn quá trình chuyển đổi số và an ninh mạng trong hệ tầng thông tin.

Chiến lược phát triển công nghệ thông tin của ngành Ngân hàng đến năm 2025, định hướng đến năm 2030 với mục tiêu thực hiện thành công chuyển đổi số trong ngành Ngân hàng. Theo đó nhấn mạnh tầm quan trọng của ATTT trong việc bảo mật, đảm bảo an ninh của hệ thống thông tin ngành ngân hàng.

Một số chỉ tiêu cụ thể như: Ít nhất 50% các nghiệp vụ được thực hiện trên môi trường số năm 2025 và đến năm 2030 đạt 70%. Chỉ tiêu về số lượng giao dịch của khách hàng trên các kênh số đạt ít nhất 70% năm 2025 và 80% vào năm 2030. Chỉ tiêu về tỷ lệ quyết định giải ngân, cho vay của Ngân hàng thương mại, công ty tài chính đối với các khoản vay nhỏ lẻ, vay tiêu dùng của khách hàng cá nhân được thực hiện số hóa: đến năm 2025 đạt tối thiểu 50% và năm 2030 đạt tối thiểu 70%.

Ngân hàng nhà nước Việt Nam ban hành Thông tư số 09/2020/TT-NHNN quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng. Thông tư quy định yêu cầu tối thiểu về đảm bảo an toàn hệ thống thông tin, trong đó phân loại cấp độ bí mật của thông tin.

Các hoạt động của ngân hàng và các tổ chức tài chính ngày càng được quy định gắt gao về các ATTT. Đặc biệt đòi hỏi sử dụng các sản phẩm, dịch vụ của bên thứ ba đạt tiêu chuẩn quốc tế. Điều này dẫn tới cuộc cạnh tranh giữa các hãng nội địa và nước ngoài ngày càng gắt gao hơn trong nhóm ngành này.

Chứng khoán và bảo hiểm – Nhóm ngành tăng trưởng đầu năm 2021

Mặc dù tình hình COVID-19 gây ra thiệt hại lớn về kinh tế cho một số ngành nghề đặc biệt du lịch và hàng không. Tuy nhiên, năm 2020 và nửa đầu năm 2021 ghi nhận sự tăng trưởng mạnh mẽ của chứng khoán, tín dụng và bảo hiểm.

Nhiều kỷ lục trên thị trường Việt Nam nửa đầu năm 2021 được ghi nhận. Sự tăng trưởng của ngành này vượt xa dự báo của các chuyên gia trước đó. VN-Index chốt phiên cuối năm 2020 ở mức 1.103,87 điểm, đầu năm 2021 ghi nhận đỉnh mới 1,308,58 điểm trong vòng 20 năm dù chịu áp lực nhỏ từ hiệu ứng “Sell in May”.

Nhận định xu hướng cuối năm 2021, các chuyên gia dự đoán thị trường vẫn tăng, tuy nhiên không quá mạnh mẽ như đợt trước, dự đoán có thể đạt 1.400 điểm năm 2021.

Số lượng tài khoản mở mới tăng chóng mặt do lãi suất ngân hàng mức thấp. Tháng 01/2021 ghi nhận 113.191 tài khoản mở mới, tháng 4/2021 ghi nhận 109.998 tài khoản mở mới.

Khối lượng giao dịch lớn trên 23.000 tỷ đồng khiến sàn HOSE liên tục rơi vào tình trạng nghẽn.

Điều này dẫn tới tiềm ẩn nguy cơ tấn công an ninh mạng rất cao với các công ty chứng khoán.

Theo báo cáo của Bộ Tài chính, tính đến hết tháng 4/2021, tổng tài sản các doanh nghiệp bảo hiểm đạt 608.324 tỷ đồng, tăng 22.72% cùng kỳ năm 2020. Doanh thu phí bảo hiểm đạt 61.208 tỷ đồng, tăng 19,12% so với cùng kỳ năm 2020.

Thị trường bảo hiểm Việt Nam có 72 doanh nghiệp, trong đó 31 doanh nghiệp bảo hiểm phi nhân thọ, 18 doanh nghiệp bảo hiểm nhân thọ, 2 doanh nghiệp tái bảo hiểm, 20 doanh nghiệp môi giới bảo hiểm và 1 chỉ nhánh doanh nghiệp bảo hiểm phi nhân thọ nước ngoài. **Trong đó 50-60% thị phần của thị trường bảo hiểm thuộc về top 5 công ty bảo hiểm:** trong đó Bảo Việt là công ty Việt Nam, các công ty còn lại chủ yếu là công ty nước ngoài như Prudential, Manulife, Dai-ichi,... Ngoài ra, còn có các công ty bảo hiểm của ngân hàng như Vietin Metlife, MB Ageas Life,...

Rủi ro an ninh mạng, rủi ro mất thông tin khách hàng và thiếu nhân lực là những khó khăn lớn nhất trong quá trình **InsurTech** của các doanh nghiệp bảo hiểm.

Doanh nghiệp lớn – Triển vọng đầu tư ATTT năm 2021

Bảng xếp hạng VNR500 năm 2020 tiếp tục ghi nhận sự lớn mạnh của các doanh nghiệp nhóm dịch vụ và công nghiệp, chiếm hơn 97.3% tỷ trọng doanh thu. Nhóm ngành nông nghiệp chỉ chiếm tỷ trọng 2.7%.

Các ngành hàng cao vượt trội so với mức trung bình của toàn bộ khối doanh nghiệp, bao gồm: cơ khí, xây dựng – vật liệu, bất động sản, tài chính, vận tải – logistics, viễn thông, công nghệ thông tin.

Các doanh nghiệp top đầu vẫn giữ vững vị thế như: Công ty TNHH Samsung Electronics Thái Nguyên, Tập đoàn Điện lực Việt Nam, Tập đoàn dầu khí Việt Nam, Tập đoàn Công nghiệp – Viễn thông Việt Nam, Tập đoàn Xăng dầu Việt Nam, Tập đoàn Vingroup – Công ty cổ phần, Tập đoàn Than & Khoáng sản Việt Nam, Công ty cổ phần Đầu tư thế giới di động.

Nhờ vào tình hình kinh doanh và tốc độ tăng trưởng khả quan năm 2021, nhóm doanh nghiệp lớn được đánh giá tiềm năng và triển vọng đầu tư ATTT trong các năm tiếp theo. Các nhóm ngành tiềm năng như: Bất động sản, Điện, Viễn thông, Công nghệ thông tin, Dầu mỏ, Bản lẻ, Than & khoáng sản.

XU HƯỚNG AN TOÀN THÔNG TIN TẠI VIỆT NAM

Nửa đầu năm sau 2021 tại Việt Nam tiếp tục chịu ảnh hưởng của dịch COVID-19, nền kinh tế và các hoạt động chưa thể hoạt động trở lại bình thường trong thời điểm này. Các xu hướng ATTT năm 2021 được dự đoán bao gồm:

Xu hướng 1:

Xu hướng Internet of Things (IoT) được dự đoán sẽ có tác động mạnh mẽ tới ATTT. Dự đoán tới năm 2025, sẽ có khoảng 30 tỉ kết nối IoT, gần 4 thiết bị IoT/ người. Xu hướng IoT có ảnh hưởng rất lớn đến ATTT trên toàn cầu và Việt Nam.

Xu hướng 2:

Theo báo của của Flexera về xu hướng sử dụng điện toán đám mây cho biết chi phí đầu tư trong năm 2021 sẽ tăng 47% và triển khai ở tất cả lĩnh vực. Các doanh nghiệp lớn tại Việt Nam như One Mount, VP Bank bắt đầu chuyển dịch lên hạ tầng Cloud, tiềm ẩn các nguy cơ tấn công an ninh mạng và lộ lọt thông tin. Cloud-based security tiếp tục là mối quan tâm cho các doanh nghiệp để phòng ngừa và đảm bảo bảo mật ATTT trên cloud.

Xu hướng 3:

Nhu cầu làm việc từ xa tăng cao trong thời điểm COVID-19 kéo theo rất nhiều rủi ro về an ninh mạng. Các xu hướng mới như Zero Trust thay cho các giải pháp VPN truyền thống đang được các công ty, doanh nghiệp quan tâm. Zero Trust được giới thiệu lần đầu tiên vào năm 2010 bởi John Kinderrvag, Forrester Research analyst với nguyên lý cơ bản “Never trust, always verify”. COVID-19 năm 2020 - 2021 đã đẩy nhanh quá trình ứng dụng Zero Trust trong bảo mật ATTT. Các giải pháp Zero Trust Network Access, Secure Access Service Edge (SASE) đang thu hút sự quan tâm trên toàn cầu.

Xu hướng 4:

Theo báo cáo “Do AI and Machine Learning make a difference in cybersecurity” của Webroot năm 2020, 96% người tham gia hiện đang sử dụng các sản phẩm Cybersecurity với AI Cybersecurity and Machine Learning.

Ứng dụng AI & Machine Learning giúp phát hiện các hành vi bất thường, phát hiện sớm, APT đang được các công ty an ninh mạng áp dụng để nâng cao trong các giải pháp ATTT như UEBA, SIEM.

Xu hướng 5:

Năm 2020 theo khảo sát CISO Effectiveness của Gartner, 78% CISOs có từ 16 công cụ an ninh mạng trở lên. Việc sử dụng nhiều hãng ATTT dẫn đến vận hành phức tạp và gia tăng nhu cầu nhân lực. Xu hướng hợp nhất và tích hợp các sản phẩm ATTT được các hãng lớn quan tâm. Điều này xuất phát từ nhu cầu giảm chi phí, giảm thiểu rủi ro khi vận hành.

PHỤ LỤC. THÔNG TIN THAM CHIẾU

Asian Development Bank, 2021, *Asian Development Outlook Report – Vietnam*, <https://www.adb.org/vi/countries/viet-nam/economy>

Flexera, 2021, *State of Cloud Report*, <https://info.flexera.com/CM-REPORT-State-of-the-Cloud>

Forrester, 2021, *New Tech: Zero Trust Network Access*, <https://stgsvcs.forrester.com/report/New+Tech+Zero+Trust+Network+Access+Q2+2021/-/E-RES161768>

Gartner, 2020, *CISO Effectiveness: A Report on the Behaviors and Mindsets That Impact CISO Effectiveness*, <https://www.gartner.com/en/newsroom/press-releases/2020-09-17-gartner-survey-reveals-only-12-percent-of-cisos-are-considered-highly-effective>

Gartner, 2021, *Top security and risk trends*, <https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021/>

Gartner, 2021, *Forecast Worldwide security and risk management*, <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem>

Ken Research, 2020, *Vietnam Cybersecurity Outlook to 2020 – Gauging the opportunities for foreign investment in the Cybersecurity industry*

Mordor Intelligence, 2021, *Asia Pacific Cyber Security market*, <https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market>

Sản phẩm dịch vụ tiêu biểu SOC kèm giá sơ bộ do Cục Tin học hoá – Bộ TT&TT niêm yết:

https://cps.mic.gov.vn/#/web/mic/san_pham?_page=1&NhomSanPham._source.PhanLoaiSanPham._source.MaMuc=dichvutieubieu&NhomSanPham._source.MaMuc=trungtamdieuhanhantoananninhmangsoc&_id=5f7ad49b21bc2b000808688f

Statista, 2020, *Global IoT Market Size 2017 – 2025*, <https://www.statista.com/statistics/976313/global-iot-market-size/>

SSI, 2020, Báo cáo ngành ngân hàng, tài chính và bảo hiểm, <http://www.ssi.com.vn/khach-hang-ca-nhan/bao-cao-nganh>

VNR500, 2020, *Bảng xếp hạng top 500 Doanh nghiệp lớn nhất Việt Nam*, <https://www.vnr500.com.vn/>