Bài tập an toàn và bảo mật thông tin

Thương Mại điện tử (Trường Đại học Thương mại)

Câu 1:

a. Trình bày các nguy cơ và đưa ra giải pháp phòng chống mất an toàn cho nhân viên các tổ chức, doanh nghiệp khi làm việc tại nhà (Work from Home – WFH) trong thời điểm dịch Covid_19. Lấy ví dụ minh họa

Trong thời điểm dịch bệnh Covid_19 và cuộc Cách mạng Công nghiệp lần thứ tư, các doanh nghiệp không ngừng đẩy mạnh chuyển đổi các hoạt động lên không gian mạng và tăng cường áp dụng công nghệ số. Vào bối cảnh đó, mô hình làm việc trực tuyến tại nhà hay làm việc từ xa trở nên phổ biến. Xử lý công việc tại nhà góp phần phòng, chống dịch đồng thời có thể mang đến nhiều thuận lợi với sự tự do, thoải mái về không gian; tiết kiệm chi phí đi lại; riêng tư và yên tĩnh… Tuy nhiên, thời cơ luôn đi kèm theo những nguy cơ.

Các công cụ trực tuyến như Gmail, Facebook, Zalo, Skype, Zoom… dường như là phương tiện không thể thiếu đối với những doanh nghiệp áp dụng chính sách làm việc từ xa cho nhân viên. Điều này tạo điều kiện cho kẻ xấu triển khai những phương thức lừa đảo dễ dàng chiếm được tài khoản làm việc của một nhân viên nào đó trong công ty. Từ đây, kẻ lừa đảo có thể thâm nhập vào mạng nội bộ của công ty và đánh cắp thông tin tài chính, dữ liệu doanh nghiệp.

Loại mã độc "tống tiền" (ransomware) doanh nghiệp đã nở rộ trong năm 2020 về đối tượng lẫn mức độ nguy hại. Chúng mở rộng đối tượng tấn công sang cả các bệnh viện, tổ chức y tế và tài chính, các cơ quan nhà máy hạ tầng thiết yếu nhằm gia tăng sức ép và giá trị tiền chuộc. Tuy vậy, mức độ hiểu biết và cảnh giác về loại mã độc này đối với khối doanh nghiệp vừa và nhỏ, siêu nhỏ vẫn còn rất hạn chế. Đại đa số các nạn nhân của ransomware có xu hướng trả tiền chuộc để lấy lại dữ liệu quan trọng. Một điểm mới của là chúng không chỉ mã hóa dữ liệu đòi tiền chuộc, mà còn tống tiền nạn nhân để khỏi bị công khai dữ liệu đó lên mạng.

Nhân viên khi làm việc từ xa cần truy cập vào cơ sở dữ liệu, File và sử dụng các phần mềm ứng dụng chuyên dụng của doanh nghiệp. Họ cũng cần trao đổi, chia sẻ tệp dữ liệu kích thước lớn trong nội bộ một cách nhanh chóng. Tuy nhiên, những tài nguyên trên

nằm trong hệ thống thông tin nội bộ của doanh nghiệp, được thiết lập bảo mật chặt chẽ và chỉ truy cập được từ các máy tính bên trong mạng LAN/WAN của doanh nghiệp đã được bộ phận quản trị hệ thống mạng thiết lập và vận hành, giám sát. Vì vậy, khi cho phép truy cập từ bên ngoài đồng nghĩa với việc "nới lỏng" an ninh và bảo mật thông tin. Điều này gây ra nguy cơ xâm nhập của người ngoài có ý định xấu vào mạng nội bộ. Giải pháp cho những nguy cơ trên, đối với tổ chức doanh nghiệp cần:

1. Quan tâm đào tạo nâng cao nhận thức bảo mật khi làm việc từ xa để nhân viên luôn kiểm tra kĩ các nguồn email nhận, không mở các tệp đính kèm khả nghi và báo ngay cho bộ phận công nghệ thông tin trong trường hợp thấy có bất thường.
2. Trang bị phần mềm chống mã độc cho máy tính và đặt chế độ tự động cập nhật phiên bản mới; cập nhật đầy đủ các bản vá của hệ điều hành và các ứng dụng phần mềm đang sử dụng; thiết lập mật khẩu đủ mạnh cho máy tính; đặt chế độ xác thực 2 yếu tố cho các tài khoản truy cập vào ứng dụng của công ty như email, lịch làm việc, ổ dữ liệu chia sẻ
3. Cần bổ sung các quy định bảo đảm an toàn, an ninh mạng trong quy trình làm việc trực tuyến như: truy cập từ xa an toàn và các yêu cầu liên quan thiết bị cá nhân, thiết lập tài khoản mới, quản lý và thiết lập mật khẩu an toàn

Đối với nhân viên, nên:

Sử dụng VPN (Virtual Private Network) để mã hóa luồng dữ liệu; cấu hình tường lửa trên máy tính để ngăn cản những truy cập trái phép bên ngoài; cài đặt những phần mềm diệt virus và cập nhật phiên bản mới thường xuyên.

Ví dụ minh họa cho việc mất an toàn và bảo mật thông tin đối với tổ chức khi áp dụng WFH:

Năm 2018, một công ty là khách hàng Athena làm trong lĩnh vực tư vấn tài chính đã triển khai làm việc từ xa cho các nhân viên kinh doanh nhưng chưa chú trọng đến an ninh mạng. Việc này dẫn đến 50.000 thông tin khách hàng và thông tin các dự án (30 dự án tiềm năng để đầu tư) bị rò rỉ gây khủng hoảng trầm trọng cho công ty, bị các đơn vị có liên quan kiện vì để dữ liệu bị đưa ra giao dịch ngoài thị trường. Thiệt hại việc mất dữ liệu này lên đến hàng tỉ đồng. Qua quá trình tìm hiểu, Athena phát hiện nhân viên công ty này truy cập và trao đổi dữ liệu khách hàng với

nhau trên môi trường không an toàn, không có biện pháp bảo mật dữ liệu, đường truyền, không có chính sách kiểm soát và ghi dấu truy cập dữ liệu của nhân viên, không có hệ thống cảnh báo rủi ro và phòng ngừa khủng hoảng. Đây chính là nguyên nhân gây mất dữ liệu mà không thể quy kết trách nhiệm cho ai được. Tham gia xử lý sự cố này, Athena đề xuất được tham gia vào ban điều hành công ty, được quyền lên kế hoạch và xây dựng các quy trình bảo đảm an ninh, an toàn, phòng chống rủi ro có thể xảy ra. Đồng thời, bố trí thêm nguồn nhân lực an ninh mạng để kiểm soát hệ thống, triển khai các phần mềm chuyên dụng giúp ban lãnh đạo giám sát theo thời gian thực.

b. Cho tình huống sau:

Các chuyên gia bảo mật tại Threat Fabric (Hà Lan) vừa phát hiện ra một loạt Trojan mới, có khả năng đánh cắp tiền trong tài khoản ngân hàng và ví tiền điện tử của người dùng. Cụ thể, mã độc này có tên Xenomorph, nhắm tới người dùng điện thoại Android. Loại mã độc này được phát hiện bên trong phần mềm có tên Fast Cleaner. Đây là một ứng dụng được quảng cáo là có khả năng dọn rác trên điện thoại Android và tăng cường hiệu quả sử dụng pin. Mã độc này tấn công người dùng bằng cách hiển thị giao diện đăng nhập giả mạo bên trên giao diện thật. Qua đó, người dùng hoàn toàn có thể mất cảnh giác và cung cấp thông tin đăng nhập tài khoản cho tin tặc. Trước khi bị gỡ khỏi kho ứng dụng CH Play. Fast Cleaner đã thu hút hơn 50.000 lượt tải xuống. Phần mềm độc hại này được thiết kế để gây khó khăn trong việc xóa bỏ.

(Theo http://antoanthongtin.vn)

- Hãy xác định và giải thích các nguy cơ mà người dùng gặp phải trong tình huống này.

Trong tình huống này, người dùng gặp phải mối đe dọa từ phần mềm Fast Cleaner mà cụ thể ở đây là mã độc Trojan bị nhiễm vào máy khi tải phần mềm này về. Người dùng đã bị ghi lại thông tin sử dụng máy tính (thao tác bàn phím, sử dụng mạng, thông tin đăng nhập, v.v...) thông qua các giao diện hiển thị đăng nhập giả mạo mà mã độc này gây ra. Theo đó, Xenomorph có thể truy cập giám soát hoạt động của nạn nhân và đưa vào đó một lớp phủ tương tự như ứng dụng gốc. Người dùng có thể nghĩ rằng họ đang làm việc trực tiếp với ứng dụng ngân hàng của mình. Trên thực tế, nạn nhân đang cung cấp thông tin tài khoản của mình cho trojan này. Sau khi được kích hoạt trên thiết bị mục tiêu, Xenomorph bắt đầu thu thập thông tin thiết bị và Tin nhắn SMS hiện có, đồng thời chặn

các thông báo và tin nhắn SMS mới. Khi người dùng cố gắng truy cập vào một trang web ngân hàng bị phần mềm độc hại nhắm mục tiêu, nó sẽ lạm dụng các tính năng Trợ năng của Android để đặt một lớp phủ trên màn hình nhằm ghi lại thông tin đăng nhập và sử dụng khả năng chặn tin nhắn SMS của nó để lấy mã thông báo xác thực 2 yếu tố.

- Hãy đưa ra các giải pháp nhằm đảm bảo an toàn cho người dùng trong tình huống này và giải thích.

  Các giải pháp:

  - Luôn luôn lựa chọn những phần mềm antivirus tốt, thường xuyên kiểm tra bằng cách quét virus cho thiết bị và sử dụng tường lửa để bảo vệ máy tính.

  - Cập nhật đầy đủ các bản vá lỗ hổng thường xuyên với máy tính Windows, để tránh trường hợp hacker lợi dụng những lỗ hổng đó xâm nhập máy tính.

  - Không tải xuống hoặc cài đặt các chương trình nếu bạn không tin tưởng hoàn toàn vào nhà xuất bản.

  - Nên hết sức cảnh giác với bất kỳ ứng dụng nào yêu cầu khả năng kiểm soát hoàn toàn thiết bị, sử dụng quyền quản trị thiết bị hoặc sử dụng tính năng trợ năng vì chúng dễ bị phần mềm độc hại lạm dụng.

Câu 2:

1. Cho nguyên bản:

   "**WATSON WON'T ALLOW THAT I KNOW ANYTHING OF ART, BUT THAT IS MERE JEALOUSY SINCE OUR VIEWS UPON THE SUBJECT DIFFER"**

   Hãy sử dụng hệ mã hóa Vigenere với K= "HOTEN" của bạn để tìm bản mã cho nguyên bản trên. (Ví dụ Họ và tên của bạn là NGUYEN VAN A thì K= "NGUYENA").

   Bài làm:

   Gọi nguyên bản là M = "**WATSON WON'T ALLOW THAT I KNOW ANYTHING OF ART, BUT THAT IS MERE JEALOUSY SINCE OUR VIEWS UPON THE SUBJECT DIFFER"**

   Khóa K = "CHUCHI"

   Dựa vào nguyên tắc mã hóa trên nguyên tắc hình vuông Vigenere bao gồm 26 hàng và 26 cột chữ cái tiếng Anh. Mỗi hàng dịch chuyển theo thứ tự của chữ cái đầu hàng, mỗi cột là

giá trị các ký tự cần mã hóa hoặc giải mã. Cụ thể, nguyên tắc này được thể hiện dưới bảng sau đây:

h	Chữ cái thuộc khóa K																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Hình 1: Hình vuông Vigenere dùng để mã hóa và giải mã

Như vậy, thực hiện mã hóa Vigenere ta được bảng sau:

Nguyên bản	W	A	T	S	O	N		W	O	N	T		A	L	L	O	W		T	H	A	T		I		K	N	O	W		A	N	Y	T	H	I	N	G
Khóa K	C	H	U	C	H	I		C	H	U	C		H	I	C	H	U		C	H	I	C		H		U	C	H	I		C	H	U	C	H	I	C	H
Bản mã	Y	H	N	U	V	V		Y	V	H	V		H	T	N	V	Q		V	O	I	V		P		E	P	V	E		C	U	S	V	O	Q	P	N

	O	F		A	R	T		B	U	T		T	H	A	T		I	S		M	E	R	E		J	E	A	L	O	U	S	Y		S	I	N	C	E	
	U	C		H	I	C		H	U	C		H	I	C	H		U	C		H	I	C	H		U	C	H	U	C	H	U	C		H	I	C	H	U	
	I	H		H	Z	V		I	O	V		A	P	C	A		C	U		T	M	T	L		D	G	H	T	Q	B	M	A		Z	Q	P	J	Y	

O	U	R		V	I	E	W	S		U	P	O	N		T	H	E		S	U	B	J	E	C	T		D	I	F	F	E	R
C	H	I		C	H	U	C	H		I	C	H	U		C	H	I		C	H	U	C	H	I	C		H	U	C	H	I	C
Q	B	Z		X	P	Y	Y	Z		C	R	V	H		V	O	M		U	B	V	L	L	K	V		K	C	H	M	M	I

Các ký hiện đặc biệt (không phải ký hiệu chữ) được thêm vào sau khi giải mã

Kết luận:

Dựa vào mã hóa Vigenere, ta thu được bản mã: “YHNUVV YVH’V HTNVQ VOIV P EPVE CUSVOQPN IH HZV, IOV APCA CU TMTL DGHTQBMA ZQPJY QBZ XPYYZ CRVH VOM UBVLLKV KCHMMT”

2. Cho bản mã:

“HSORRIWBAFSIAGRNOIWHOEISTOIENIEILSNIFNTEIRCNDCANMKFSICHROES CLASGENOPCYOVNNCEOLO”. Biết bản mã được mã hóa với hệ mã hóa hàng rào với K= “5”. Hãy tìm nguyên bản của bản mã trên?

Bài làm:

Thực hiện giải mã theo các bước sau:

Bước 1: Đếm tổng số ký tự của bản mã ta được: 79 ký tự. Lấy tổng số ký tự này chia cho giá trị của khóa K (=5) được 16 dư 1.

Bước 2: Viết lại bản mã vào bảng gồm 5 cột và 16 hàng, các ký tự của bản mã lần lượt từ trái sang phải được viết theo thứ tự từng cột (từ trên xuống dưới) sao cho vừa với giới hạn cột và hàng của bảng. Cụ thể như bảng dưới đây:

1	2	3	4	5
H	O	L	M	E
S	I	S	K	N
O	W	N	F	O
R	H	I	S	P
R	O	F	I	C
I	E	N	C	Y
W	I	T	H	O
B	S	E	R	V
A	T	I	O	N
F	O	R	E	N
S	I	C	S	C
I	E	N	C	E
A	N	D	L	O
G	I	C	A	L

R	E	A	S	O
N	I	N	G	

Bước 3: Từ bước 2, ta thu được nguyên bản:
“HOLMESISKNOWNFORHISPROFICIENCYWITHOBSERVATION FORENSICSCIENCEANDLOGICALREASONING”

Có thể tách nguyên bản này như sau để hiểu rõ ràng hơn về ý nghĩa: HOLMES IS KNOWN FOR HIS PROFICIENCY WITH OBSERVATION FORENSIC SCIENCE AND LOGICAL REASONING”

3. Tìm khóa

Cho trước cặp số nguyên tố: (p = 41, q = 23). Hãy chọn số e và sử dụng thuật toán RSA để tìm cặp khóa công khai, khóa bí mật và $\Phi(n)$.

Bài làm:

Tính N = p x q = 41 x 23 = 943

Tính $\Phi(n) = (p - 1) \times (q - 1) = 40 \times 22 = 880$

Chọn e: gcd(e, 880) = 1 và 1< e < 880; lấy e = 37

Tìm d sao cho d x e ≡ 1 mod 880 và d < = 943 nghĩa là tích số d x e chia cho tích số (P-1)(Q-1) = 880 có số dư là 1, hay là (d*e - 1) chia hết cho 880

Ta dùng phương pháp thử và loại dần các số nguyên X sao cho có được: d = [X*(P-1)(Q-1) +1]/e là một số nguyên, d được gọi là số mũ giải mã hay số d.

Thử trong khoảng X = 1 tới X = 15 ta thu được d = 333 (X = 14)

Công bố khóa công khai Kc = {19, 943}

Giữ riêng tư khóa bí mật Kr = {37, 943}

---Hết---