XÂY DỰNG CHÍNH SÁCH MẬT KHẨU AN TOÀN, DỄ SỬ DỤNG - XU HƯỚNG BẢO MẬT THÔNG TIN HIỆN ĐẠI TRONG MỘT HỆ THỐNG

NGUYỄN THỊ THANH BÌNH*

Ngày nhận: 1/3/2019
Ngày phản biện: 15/4/2019
Ngày duyệt đăng: 24/5/2019

Tóm tắt: Vấn đề an toàn và bảo mật thông tin là vấn đề quan trọng trong thời đại công nghệ thông tin hiện nay. Người dùng trong các hệ thống thường sử dụng biện pháp truyền thống là mật khẩu để bảo vệ tài nguyên và dữ liệu của mình. Bài báo đề cập đến xu thế xây dựng một chính sách mật khẩu an toàn và dễ sử dụng cho người dùng trong hệ thống như: thành phần, độ phức tạp, thời hạn sử dụng, chính sách khóa và cảnh báo mật khẩu...

Từ khóa: an toàn thông tin, dữ liệu, hệ thống, mật khẩu, chính sách mật khẩu, độ phức tạp.

BUILDING A SAFE AND EASY-TO-USE PASSWORD POLICY - MODERN SECURITY TRENDS IN A SYSTEM

Abstract: Information security is an important issue in the era of information technology today. Users in a system often use traditional methods as passwords to protect their resources and data. The article mentioned the trend of building a safe and easy-to-use password policy for users in the system such as components, complexity, expiry dates, lock policies and password alerts...

Keywords: secure information, data, system, password, password policy, password's complexity.

1. Đặt vấn đề

Ngày nay, xã hội loài người ngày càng phụ thuộc nhiều vào các hệ thống mạng và hệ thống thông tin. Trong xu thế hội nhập kinh tế thế giới và toàn cầu hóa, công nghệ thông tin và truyền thông (CNTT&TT) đã trở thành một động lực quan trọng để thúc đẩy sự phát triển của toàn bộ xã hội và đang làm biến đổi sâu sắc đời sống kinh tế, văn hóa, xã hội của thế giới hiện đại. Việc ứng dụng viễn thông và CNTT hiện đại đang là nhu cầu, là xu thế tất yếu trên con đường phát triển của mọi quốc gia.

Bên cạnh những ưu thế do viễn thông và CNTT mang lại, thì mặt trái bộc lộ những hiểm họa và nguy cơ mất an toàn, an ninh thông tin trong hệ thống. CNTT&TT hàng năm luôn phải đối mặt với nhiều loại hình tấn công trên mạng ngày càng thường xuyên hơn như làm biến dạng trang tin, lừa đảo trên mạng, tấn công từ chối dịch vụ, phát tán mã độc hại và virút máy tính, thư rác, đánh cắp thông tin, phá hoại dữ liệu, làm gián đoạn và phá rối hoạt động của các hệ thống thông tin, phần mềm gián điệp, tấn công hệ thống ngân hàng và mạng bán hàng trực tuyến, nhắn tin lừa đảo, đe dọa, tống tiền,... Chính vì vậy, an toàn thông tin ngày càng trở thành một vấn đề nóng vì có ảnh hưởng lớn đến sự phát triển của CNTT&TT và có tác động không nhỏ đến mọi lĩnh vực.

Tóm lại, sự phát triển không ngừng của lĩnh vực CNTT đã tạo điều kiện thuận lợi cho mọi mặt của đời sống xã hội, bên cạnh những mặt thuận lợi, cũng có nhiều nguy cơ về mất an toàn thông tin trong hệ thống.

2. Sự cần thiết của việc xây dựng chính sách bảo mật thông tin cho hệ thống

Các hệ thống luôn bị đe dọa bởi các nguy cơ mất an toàn thông tin. Một trong những công việc để bảo vệ hệ thống là làm sao giúp hệ thống tránh khỏi các nguy cơ đó. Có 4 loại mối đe dọa an toàn thông tin trong một hệ thống:

Chặn bắt (Interception): là mối đe dọa mà các thành viên không nằm trong hệ thống, không có quyền truy cập vào hệ thống mà bằng cách nào đó như: tấn công mật khẩu, tấn công bị động,...lại có thể truy cập đến các dịch vụ hay các dữ liệu của hệ thống, "nghe trộm" thông tin đang được truyền đi trên hệ thống hoặc làm hệ thống ngưng trệ.

* *Trường Đại học Công đoàn*

Đứt đoạn (Interruption): là mối đe dọa mà làm cho dịch vụ hay dữ liệu của hệ thống bị mất mát, bị hỏng, không thể truy cập hay không thể dùng được nữa.

Thay đổi (Modification): là mối đe dọa làm cho dữ liệu của hệ thống có hiện tượng thay đổi hay các dịch vụ của hệ thống bị can thiệp nên chúng không còn giữ được các đặc tính ban đầu.

Giả mạo (Fabrication): là mối đe dọa hiện tượng thêm vào dữ liệu ban đầu các dữ liệu hay hoạt động đặc biệt mà không thể nhận biết được để ăn cắp dữ liệu của hệ thống.

Nguy cơ hệ thống mất an toàn thông tin hệ thống là do nhiều nguyên nhân hoặc có thể đến từ nhiều đối tượng khác nhau như: môi trường (thời tiết ẩm thấp ảnh hưởng đến phần cứng), người dùng (người dùng đang làm việc, người dùng đã nghỉ việc, những đối thủ cạnh tranh trực tiếp), đối tượng tấn công (tội phạm máy tính - hacker mũ đen)... Thiệt hại từ những vụ tấn công vào các hệ thống bị mất an toàn thông tin là rất lớn, đặc biệt là những hệ thống thông tin thuộc lĩnh vực kinh tế, an ninh, quốc phòng...

Hiện trạng mất an toàn thông tin đối với hệ thống của các tổ chức nhà nước, chính phủ, doanh nghiệp, cá nhân không còn là nguy cơ rủi ro nữa mà đang là vấn đề nhìn thấy ở mức độ nghiêm trọng. Để làm rõ mức độ nghiêm trọng của mất an toàn thông tin chúng ta cần nhìn mấy vụ việc điển hình đã xảy ra gần đây. Điển hình là Hãng hàng không quốc gia Việt Nam vừa bị tin tặc tấn công hệ thống thông tin của hãng và lấy đi dữ liệu của 400.000 tài khoản khách hàng, khiến hệ thống thông tin, quầy thủ tục tại các sân bay tê liệt; ảnh hưởng nghiêm trọng đến an toàn bay, chậm chuyến, thậm chí ảnh hưởng đến tính mạng của hành khách... Hay trường hợp khách hàng của ngân hàng VCB, VPB bị mất tiền trong tài khoản không rõ nguyên nhân... Chỉ trong chưa đầy một tháng, nhiều vụ việc liên quan đến vấn đề tiền gửi tài khoản của khách hàng "không cánh mà bay". Trên thực tế, nhiều người dân gửi tiền vào tài khoản ngân hàng nhưng vì quy trình an toàn thông tin chưa được chú trọng nên nhiều khi bị lộ thông tin, thậm chí mất tiền oan không rõ lý do.

Một hệ thống an toàn là một hệ thống đảm bảo được những yếu tố bảo mật về dữ liệu, tài nguyên và danh tiếng như sau:

Yếu tố đầu tiên phải nói đến là dữ liệu, dữ liệu là một trong những thông tin quan trọng của mọi hệ thống. Khi đó, nếu hệ thống không có những chính sách bảo vệ thông tin một cách toàn diện, dữ liệu đó rất có thể bị đánh cắp bất kì lúc nào. Thông thường yêu cầu về bảo mật được coi là yêu cầu quan trọng đối với dữ liệu được lưu trữ trong hệ thống.

Yếu tố thứ hai là về tài nguyên hệ thống như: phần cứng, phần mềm ứng dụng... Sau khi những kẻ tấn công đã làm chủ được hệ thống chúng sẽ sử dụng các tài nguyên này để phục vụ cho các mục đích cá nhân, thậm chí làm cho hệ thống bị tê liệt, không có khả năng tiếp tục hoạt động.

Yếu tố thứ ba là danh tiếng: một khi dữ liệu bị đánh cắp thì việc nghi ngờ nhau trong hệ thống là điều không tránh khỏi, vì vậy sẽ ảnh hưởng đến danh tiếng của hệ thống rất nhiều.

Trước những hiểm họa tinh vi từ sự phát triển của mạng Internet và các thiết bị kỹ thuật số hiện đại, các sự cố về thông tin ngày càng xảy ra nhiều, nghiêm trọng và rất khó để tìm ra các hướng giải quyết. Việc xây dựng những chính sách bảo mật thông tin, an toàn thông tin cho hệ thống là việc làm vô cùng cần thiết.

Sau đây là một số phương thức bảo đảm an toàn, bảo mật thông tin truyền thống trong một hệ thống:

Mật mã (Cryptography): là việc thực hiện chuyển đổi dữ liệu theo một quy tắc nào đó, dữ liệu sẽ được mã hóa thành dạng mới mà kẻ tấn công không nhận biết được.

Xác thực (Authentication): là các thao tác để nhận dạng người dùng, nhận dạng client hay server...

Ủy quyền (Authorization): chính là việc phân định quyền hạn cho mỗi thành phần đã đăng nhập thành công vào hệ thống. Quyền hạn này là các quyền sử dụng dịch vụ, truy cập dữ liệu...

Kiểm toán (Auditing): là các phương pháp để xác định được người dùng đã truy cập đến dữ liệu nào và bằng cách nào.

Trong các phương thức nói trên, phương thức xác thực bằng mật khẩu được sử dụng rộng rãi và phổ biến nhất trong các hệ thống hiện nay. Tuy nhiên, phương thức xác thực này vẫn còn tồn tại những lỗ hổng và có khả năng bị phá vỡ. Vì vậy, xu hướng xây dựng một chính sách mật khẩu an toàn, dễ sử dụng cho hệ thống đang ngày càng được quan tâm và phát triển mạnh mẽ.

3. Xây dựng chính sách mật khẩu để bảo mật thông tin cho hệ thống

Hầu hết người dùng đăng nhập vào máy tính cá nhân cục bộ của họ hay các máy tính từ xa hoặc người dùng đăng nhập vào một hệ thống thường sử dụng kết hợp tên người dùng (account) và một mật khẩu (password) được nhập từ bàn phím. Mặc dù có

nhiều kỹ thuật khác để thẩm định, như các thẻ thông minh, sinh trắc học, hay mật khẩu mật..., nhưng hầu hết các hệ thống vẫn sử dụng mật khẩu truyền thống để đảm bảo an toàn thông tin cho hệ thống của mình.

Việc tìm ra một mật khẩu tốt và xây dựng được chính sách mật khẩu cho hệ thống là một vấn đề quan trọng và cần thiết mà một hệ thống nên làm. Một mật khẩu tốt phải là mật khẩu có mức độ phức tạp nhất định liên quan đến các đặc điểm như: độ dài, thành phần ký tự, nội dung,... để làm cho mật khẩu trở nên khó đoán hơn hơn trước kẻ tội phạm khi muốn xâm nhập vào hệ thống.

Việc xây dựng một chính sách mật khẩu tốt cho hệ thống có thể giúp ngăn cản kẻ tấn công đóng vai người dùng hợp pháp và bằng cách đó có thể ngăn chặn việc mất dữ liệu, thông tin quan trọng đảm bảo an toàn thông tin cho hệ thống.

Chính sách mật khẩu thường là các quy định của hệ thống mà người sử dụng cần phải biết rõ và tuân thủ theo để có thể chính thức tham gia vào hệ thống. Chính sách mật khẩu là một bộ quy tắc được thiết kế để tăng cường bảo mật hệ thống bằng cách khuyến khích người dùng sử dụng mật khẩu mạnh và sử dụng chúng đúng cách. Hiểu được chính sách mật khẩu của một hệ thống là bước đầu tiên để người dùng có thể tham gia vào hệ thống đó.

Các nội dung của chính sách mật khẩu của một hệ thống bao gồm:

Thành phần của mật khẩu

Thành phần của mật khẩu quyết định độ phức tạp của mật khẩu. Nếu mật khẩu chứa các ký tự đặc biệt, đa dạng và có độ phức tạp cao thì mật khẩu đó sẽ có tính bảo mật cao và được coi làm một mật khẩu mạnh. Một số qui định về thành phần của mật khẩu như sau:

- Bao gồm cả chữ hoa và chữ thường
- Bao gồm một hoặc nhiều số
- Bao gồm các ký tự đặc biệt, chẳng hạn như @, #, $
- Không sử dụng các từ được tìm thấy trong danh sách đen mật khẩu
- Không sử dụng tên công ty hoặc viết tắt
- Không sử dụng các mật khẩu phù hợp với định dạng ngày tháng theo lịch, số biển số xe, số điện thoại, hoặc các số phổ biến khác
- Mật khẩu không chứa thông tin cá nhân như: tên riêng, ngày sinh, số điện thoại cầm tay,...
- Sử dụng các mật khẩu khác nhau cho các tài khoản khác nhau
- Không nên sử dụng mật khẩu quá dài vì rất khó nhớ
- Không thay đổi mật khẩu thường xuyên
- Không sử dụng mật khẩu đã sử dụng trước đó
- Không ghi nhớ mật khẩu trên mọi hình thức: ghi ra giấy, lưu trên các trình duyệt,...

Tuy nhiên, mật khẩu cũng không nên có thành phần quá phức tạp vì người dùng sẽ dễ quên. Vì

Bảng 1: Thời gian tấn công mật khẩu phụ thuộc vào độ dài mật khẩu [1]

Password Length	Charset	Num Users	Cracking Speed	Days to Crack	Years to Crack	Passwords per day	Passwords per year
8	36	10000	2.00E+10	0.00	0.00	10,000.00	10,000.00
8	62	10000	2.00E+10	0.13	0.00	10,000.00	10,000.00
8	96	10000	2.00E+10	4.17	0.01	2,395.38	10,000.00
9	36	10000	2.00E+10	0.06	0.00	10,000.00	10,000.00
9	62	10000	2.00E+10	7.83	0.02	1,276.49	10,000.00
9	96	10000	2.00E+10	400.77	1.10	24.95	9,107.42
10	36	10000	2.00E+10	2.12	0.01	4,726.27	10,000.00
10	62	10000	2.00E+10	485.71	1.33	20.59	7,514.84
10	96	10000	2.00E+10	38,474.11	105.41	0.26	94.87
11	36	10000	2.00E+10	76.17	0.21	131.29	10,000.00
11	62	10000	2.00E+10	30,113.75	82.50	0.33	121.21
11	96	10000	2.00E+10	3,693,514.64	10,119.22	0.00	0.99
12	36	10000	2.00E+10	2,742.12	7.51	3.65	1,331.09
12	62	10000	2.00E+10	1,867,052.52	5,115.21	0.01	1.95
12	96	10000	2.00E+10	354,577,405.86	971,444.95	0.00	0.01
13	36	10000	2.00E+10	98,716.28	270.46	0.10	36.97
13	62	10000	2.00E+10	115,757,256.52	317,143.17	0.00	0.03
13	96	10000	2.00E+10	34,039,430,962.76	93,258,714.97	0.00	0.00
14	36	10000	2.00E+10	3,553,786.00	9,736.40	0.00	1.03
14	62	10000	2.00E+10	7,176,949,904.32	19,662,876.45	0.00	0.00
14	96	10000	2.00E+10	3,267,785,372,425.43	8,952,836,636.78	0.00	0.00

[1] Password Complexity Requirements, http://bugcharmer.blogspot.com/2012/09/password-complexity-requirements.html

vậy, chính sách mật khẩu thông dụng hiện nay thường qui định thành phần của mật khẩu như sau: mật khẩu có độ dài tối thiểu 6 ký tự, chứa ít nhất với một chữ hoa và một chữ thường, một ký tự đặc biệt và một chữ số.

Độ dài của mật khẩu

Mật khẩu được coi là mạnh hay có độ phức tạp cao là mật khẩu đảm bảo được 2 yếu tố: độ dài của mật khẩu và các ký tự chứa trong nó. Chính vì vậy mật khẩu càng dài thì tính an toàn càng cao.

Theo một nghiên cứu về độ dài của mật khẩu của tác giả Steven Alexander Dưới đây là một bảng dữ liệu mô tả khoảng thời gian để tấn công mật khẩu không có một chiều dài nhất định và bao nhiêu mật khẩu mỗi ngày hoặc năm mà kẻ tấn công có thể phục hồi trong một cuộc tấn công offline. Tác giả cho rằng có 10 nghìn người dùng và kẻ tấn công có thể đoán được 20 tỷ mật khẩu mỗi giây. (xem *bảng 1*)

Tác giả nhấn mạnh độ dài của mật khẩu càng lớn thì sẽ mang lại ít hơn một mật khẩu mỗi ngày cho kẻ tấn công. Dựa vào các con số ở bảng trên, tác giả đã chỉ ra rằng mật khẩu nên có ít nhất 10-12 ký tự.

Tuy nhiên, độ dài của mật khẩu sẽ ảnh hưởng đến khả năng nhớ của người dùng. Nếu mật khẩu dài quá, người dùng sẽ rất khó nhớ, dẫn đến việc truy cập vào hệ thống sẽ bị gián đoạn. Vì vậy, cần xác định độ dài của mật khẩu có độ dài phù hợp để đảm bảo tính an toàn cũng như dễ sử dụng.

Các chính sách mật khẩu thường có yêu cầu về độ dài tối thiểu của mật khẩu là 6 ký tự.

Danh sách đen mật khẩu

Danh sách đen mật khẩu là danh sách mật khẩu luôn bị cấm sử dụng. Danh sách đen chứa mật khẩu không an toàn vì một hoặc nhiều lý do, chẳng hạn như dễ đoán, theo một khuôn mẫu chung hoặc tiết lộ công khai trước những vi phạm dữ liệu trước đó.

Các mật khẩu trong danh sách đen chắc chắn là một mật khẩu yếu. Một mật khẩu yếu là một mật khẩu ngắn, phổ biến, một mặc định của hệ thống cung cấp, hoặc một thứ gì đó có thể bị đoán ra nhanh chóng như các từ trong từ điển, tên riêng, những từ dựa trên tên người dùng hoặc những biến thể thông thường của các từ đó. Mật khẩu có thể bị dễ dàng đoán được dựa trên những hiểu biết về người dùng đó, như ngày tháng năm sinh và tên thú nuôi, cũng bị xem là yếu...

Các ví dụ về mật khẩu yếu:

- admin—quá dễ đoán
- abc123—quá dễ đoán
- minh—tên riêng thông thường
- password—đoán ra dễ dàng, rất thường dùng
- p@$$VV0rd — leet và mật mã bằng ký tự đơn giản đều đã được lập trình trước trong các công cụ bẻ khóa
- 12/3/75—ngày tháng, có thể quan trọng đối với cá nhân đó
- December12—Sử dụng ngày bắt buộc phải đổi mật khẩu là rất phổ biến
- asdf—chuỗi ký tự kế nhau trong nhiều loại bàn phím
- qwerty—một chuỗi ký tự kế nhau trong nhiều loại bàn phím
- aaaa—ký tự lặp đi lặp lại, dễ đoán ra.

Thời hạn mật khẩu

Để đảm bảo tính an toàn của mật khẩu, một hệ thống cần phải đưa ra một thời hạn sử dụng mật khẩu nhất định, điều này đồng nghĩa với việc không thể dùng một mật khẩu vĩnh viễn. Thời hạn này sẽ xác định người dùng có thể giữ mật khẩu bao lâu trước khi họ phải thay đổi nó. Mục đích là để buộc người dùng thay đổi mật khẩu của họ theo định kỳ.

Thời hạn mật khẩu được xác định bởi 2 yếu tố: Tuổi thọ tối đa và tuổi thọ tối thiểu.

Tuổi thọ tối đa của mật khẩu chỉ ra một mật khẩu có thể được sử dụng bao nhiêu ngày trước khi người dùng bị yêu cầu thay đổi nó. Giá trị này nằm giữa 0 đến 99; nếu nó được thiết lập là 0 thì các mật khẩu không bao giờ hết hiệu lực. Thiết lập giá trị này quá thấp có thể là nguyên nhân gây mất tác dụng cho người dùng; ngược lại giá trị này quá cao hoặc vô hiệu hóa chúng thì nó sẽ cho phép các kẻ tấn công có thêm thời gian để xác định các mật khẩu. Với hầu hết các tổ chức, giá trị này được thiết lập là 42 ngày.

Tuổi thọ tối thiểu chỉ ra bao nhiêu ngày một người dùng phải giữ các mật khẩu mới trước khi họ có thể thay đổi chúng. Thiết lập này được thiết kế để người dùng không thể nhanh chóng thiết lập lại các mật khẩu và sau đó thay đổi lại mật khẩu cũ của họ. Giá trị của thiết lập này có thể từ 0 đến 999; nếu nó được thiết lập bằng 0 thì người dùng có thể thay đổi ngay lập tức các password mới. Với hầu hết các tổ chức, giá trị này là 2 ngày.

Vấn đề về thời hạn mật khẩu thường đối mặt với một số phản đối. Một số người dùng khó có thể sáng tạo mật khẩu "tốt" cũng dễ nhớ, vì vậy nếu người dùng phải chọn nhiều mật khẩu vì phải thay đổi mật khẩu thường xuyên, họ sẽ sử dụng nhiều mật khẩu yếu hơn dẫn đến việc mật khẩu sẽ không còn an toàn.

Các khía cạnh của con người về mật khẩu cũng

phải được xem xét. Không giống máy tính, người dùng con người không thể xóa một bộ nhớ và thay thế nó bằng bộ nhớ khác. Do đó, thường xuyên thay đổi mật khẩu đã ghi nhớ là một sự căng thẳng trong bộ nhớ của con người, và hầu hết người dùng sử dụng để chọn một mật khẩu tương đối dễ đoán. Người dùng thường được khuyên sử dụng các thiết bị nhớ để nhớ các mật khẩu phức tạp. Tuy nhiên, nếu mật khẩu phải được thay đổi nhiều lần, tính nhớ sẽ vô dụng vì người dùng sẽ không thể nhớ mật khẩu nào để sử dụng. Chính vì vậy, lợi ích của việc sử dụng thời hạn mật khẩu vẫn còn gây tranh cãi. Một số hệ thống yêu cầu người dùng thay đổi mật khẩu theo định kỳ, thường là 90 hoặc 180 ngày.

Cảnh báo và khóa tài khoản

Khi người dùng không nhớ mật khẩu và cố gắng nhiều lần để đăng nhập vào một hệ thống thì hệ thống đó cần đưa ra cảnh báo không cho tiếp tục đăng nhập vào hệ thống và hơn nữa cần có chính sách khóa tài khoản của người dùng đó tạm thời trong một khoảng thời gian nhất định để đảm bảo tính bảo mật của hệ thống.

Vấn đề cảnh báo và khóa tài khoản tạm thời của một hệ thống phải bao gồm ngưỡng khóa hoặc số lần thử có thể được thực hiện trước khi khóa. Qua các nghiên cứu về khả năng phục hồi trí nhớ để khôi phục lại mật khẩu đăng nhập của người dùng, số lần thử tối đa để đăng nhập hệ thống có thể dao động từ 3 đến 5 lần là phù hợp. Thời gian khóa tạm thời của hệ thống có thể dao động từ 15 phút đến 30 phút. Tùy vào mức độ quan trọng của hệ thống thời gian tạm khóa có thể nhiều hơn hoặc thậm chí có thể khóa vĩnh viễn, tương đương với việc tài khoản sẽ bị xóa.

Sau đây là một minh họa về chính sách mật khẩu của của một hệ thống có tính bảo mật cao:

· Độ dài tối thiểu của mật khẩu là 8 ký tự

· Mật khẩu không nằm trong danh sách đen

· Thành phần của mật khẩu: Chứa ít nhất 1 ký tự hoa, 1 ký tự thường, 1 ký tự đặc biệt và 1 chữ số

· Thời hạn của của mật khẩu là 90 ngày

· Chính sách cảnh báo sau 3 lần đăng nhập hệ thống không thành công

· Chính sách khóa tài khoản sau 5 lần đăng nhập hệ thống không thành công

Tóm lại, những vấn đề an ninh và an toàn thông tin là những vấn đề rất cần thiết khi phân tích và thiết kế một hệ thống. Việc thiết lập một chính sách mật khẩu an toàn, dễ sử dụng và hợp lý đối với người dùng đang là xu hướng bảo mật thông tin hiện đại của các hệ thống trong thời kỳ CNTT phát triển mạnh mẽ. Các nhà thiết kế hệ thống và quản trị viên hệ thống cần phải thường xuyên cập nhật mới lại chính sách mật khẩu của họ để có thể đối phó với các cách tấn công kiểu mới vào hệ thống, ngăn chặn được các nguy cơ mất an toàn thông tin của hệ thống. Người dùng cũng cần có ý thức hơn trong việc tìm hiểu chính sách mật khẩu, tuân thủ mọi qui định của hệ thống và sử dụng mật khẩu đủ mạnh để đảm bảo an toàn cho dữ liệu của cá nhân cũng như dữ liệu của hệ thống mà mình tham gia. ❑

Tài liệu tham khảo

1. Đề tài NCKH cấp cơ sở của BM Tin học năm 2018, *"Phương pháp xác thực người dùng trong quản lý lớp học trực tuyến các học phần Tin học tại Trường Đại học Công đoàn"*
2. Độ mạnh của mật khẩu, https://vi.wikipedia.org/wiki/%C4%90%E1%BB%99_m%E1%BA%A1nh_c%E1%BB%A7a_m%E1%BA% ADt_kh%E1%BA%A9u.
3. Những khái niệm cơ bản về An toàn thông tin mạng, https://securitydaily.net/an-toan-thong-tin-mang/ (Ngày cập nhật 20/10/2018).
4. Password Complexity Requirements, http://bugcharmer.blogspot.com/2012/09/password-complexity-requirements.html (Ngày cập nhật 17/9/2012).
5. Bùi Văn Nam, Giải pháp bảo đảm an toàn thông tin trong tình hình hiện nay, http://nhandan.com.vn/xahoi/item/34094402-giai-phap-bao-dam-an-toan-thong-tin-trong-tinh-hinh-hien-nay.html (Ngày cập nhật 14/9/2017).
6. Thiết lập hệ thống password an toàn, https://quantrimang.com/thiet-lap-he-thong-password-an-toan-35212 (Ngày cập nhật (29/1/2017).
7. Mai Hoa, 6 cách tạo mật khẩu an toàn nhất, http://xahoithongtin.vnmedia.vn/trai-nghiem/download/201406/6-cach-tao-mat-khau-an-toan-nhat-486601/ (Ngày cập nhật ngày 17/6/2014).

XU HƯỚNG CHUYỂN DỊCH CƠ CẤU...

(Tiếp theo trang 74)

triển kinh tế - xã hội. Trường Đại học Kinh tế quốc dân, Hà Nội.

5. Tổng cục thống kê (08:34 28/12/2018). *Tổng quan kinh tế - xã hội Việt Nam năm 2018*. Khai thác từ http://www.gso.gov.vn/default.aspx?tabid=382&idmid=&ItemID=19041
6. Tổng cục thống kê (14:00 27/12/2017). *Thông cáo báo chí tình hình kinh tế - xã hội năm 2017*. Khai thác từ https://www.gso.gov.vn/default.aspx?tabid= 382&idmid=2&ItemID=18667
7. Trần Văn Thọ (2018). *Tiềm năng phát triển tốc độ cao của kinh tế Việt Nam*, Khai thác từ www.viet-studies.net/kinhte/TranVanTho _PhatTrienTocDoCao_DD.pdf
8. Nguyễn Trần Quế (chủ biên) (2004), *Chuyển dịch cơ cấu kinh tế Việt Nam trong những năm đầu thế kỷ 21*, NXB Khoa học Xã hội, Hà Nội.