MỘT SỐ PHƯƠNG PHÁP BẢO MẬT DỮ LIỆU VÀ AN TOÀN CHO MÁY CHỦ

NGUYỄN THỦY KHÁNH*

Ngày nhận: 4/9/2019
Ngày phản biện: 28/11/2019
Ngày duyệt đăng: 25/12/2019

Tóm tắt: Những phát triển nhanh chóng của các công nghệ kỹ thuật số trên Internet vừa tạo ra cơ hội, động lực để phát triển, nhưng cũng làm gia tăng các lỗ hổng tạo điều kiện cho tội phạm mạng lợi dụng để tiến hành các hoạt động ngày càng tinh vi: tấn công vào các hệ thống thông tin quan trọng của các Cơ quan Chính phủ, các Bộ, Ngành và các đơn vị, tổ chức để xâm nhập và sử dụng trái phép dữ liệu với mục tiêu đánh cắp thông tin, dữ liệu cá nhân của người dùng; giả mạo các cơ quan, tổ chức, cá nhân để bôi nhọ, nói xấu và phát tán thông tin độc hại trên mạng; đặc biệt là tấn công lây nhiễm mã độc sử dụng trí tuệ nhân tạo (AI); tấn công vào hạ tầng, thiết bị IoT, đô thị thông minh và lợi dụng các hạ tầng, thiết bị này để thực hiện các mục đích xấu.

Mỗi năm có hàng nghìn trang mạng của Việt Nam bị tin tặc xâm nhập nhằm đánh cắp thông tin, chiếm quyền điều khiển, thay đổi, chèn thêm nội dung, cài cắm mã độc... Riêng đối với các trường đại học, các thông tin cá nhân của sinh viên, cơ sở dữ liệu điểm và nguồn tài nguyên học liệu là mỏ vàng cho các tin tặc.

Từ khóa: An ninh mạng, bảo vệ, giáo dục.

PROTECTING UNIVERSITIES AND SOLVING CYBER SECURITY ISSUES

Abstract: We live in a world where technology is rapidly taking over our lives, like literally. The Internet has made connectivity seamless across various platforms. The ideal of the world becoming a global village has in actuality been achieved. Criminals are continually attacks on important information systems of Government agencies, ministries, branches and units and organizations to illegally stealing, exploiting, and holding to ransom the most prized and valuable asset of any organisation – its data. No organisation today is immune from the threat of cyber attacks. Essentially, information stealers, Trojans are a variant of malware originally designed to target the banking industry, especially malware infection using artificial intelligence (AI); attacks on infrastructure, IoT devices, smart cities and taking advantage of these infrastructure and devices to perform malicious purposes.

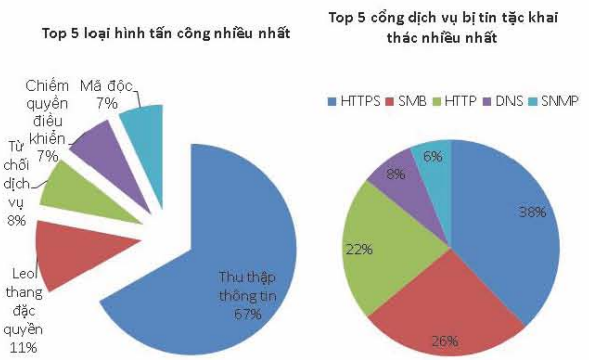
Every year, thousands of Vietnamese websites are hacked to steal information, gain control, change, add content, install malicious code... In particular, our universities and institutes of higher learning have become prime targets for bad actors looking to exfiltrate the vast amounts of sensitive data and valuable research information they hold.

Keywords: Cyber security, protect, education.

1. Đặt vấn đề

Trong thời đại kết nối internet qua các thiết bị thông minh, vấn đề an toàn và bảo mật cho dữ liệu kỹ thuật số ngày càng quan trọng và phức tạp hơn bao giờ hết. 36% số trường đại học bị một đợt tấn công trên mạng mỗi giờ [1]. Năm 2016, theo báo cáo về Đạo luật Clery; 78% tội phạm hướng đến sinh viên và nhân viên trong trường đại học [2]. Giáo dục bậc cao là khu vực chiếm 17% các vụ xâm nhập dữ liệu với thông tin cá nhân bị đánh cắp, chỉ đứng sau ngành y tế [3]; 37% lãnh đạo giáo dục bậc cao cho biết cửa ra vào và khóa trong nhà trường chưa được thiết kế đúng chuẩn an toàn và an ninh [4]. Không có tổ chức nào ngày nay miễn nhiễm với các mối đe dọa của các cuộc tấn công mạng.

Biểu đồ: Top 5 loại hình tấn công nhiều nhất và Top 5 cổng dịch vụ bị tin tặc khai thác nhiều nhất

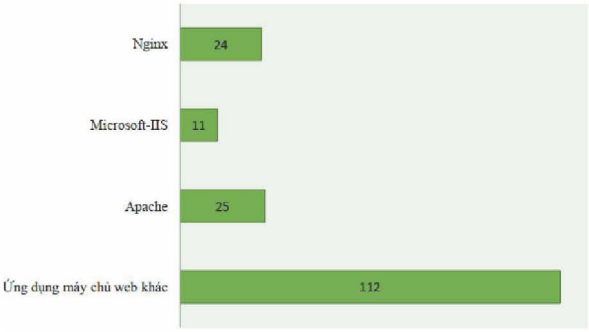


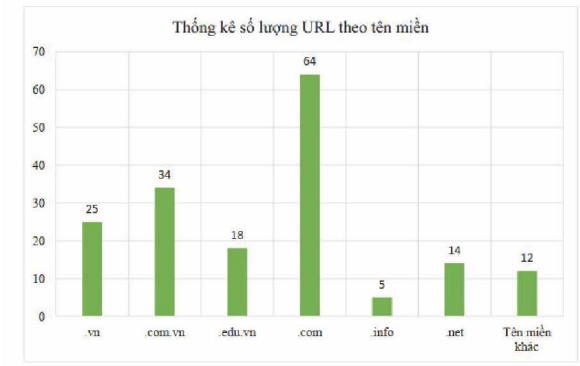
(Nguồn: Số liệu khảo sát Tổng kết an ninh mạng năm 2018 và dự báo xu hướng 2019 của BKAV)

* Trường Đại học Công đoàn

Việt Nam xếp thứ 11 trong số các nước bị hack website nhiều nhất trên thế giới. Theo đó, trung bình mỗi tháng có tới 1000 website bị xâm phạm - tương đương 35 trang web bị hack mỗi ngày [6]. Trên không gian mạng đang tồn tại nhiều trang web Việt Nam (bao gồm cả những trang web sử dụng dịch vụ máy chủ nước ngoài) bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc (gần đây nhất là cài đặt và phát tán mã độc để đào tiền ảo); lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động (như lỗ hổng trên trình duyệt hay các thành phần mở rộng của trình duyệt mà người dùng sử dụng v.v...). Trong một tuần từ 16/7/2018 đến ngày 22/7/2018, Cục ATTT ghi nhận có ít nhất 172 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache ...) và nhà cung cấp cụ thể như sau:

Thống kê số lượng URL bị tấn công theo ứng dụng máy chủ web [7]





Năm 2018, thiệt hại do tin tặc gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 14.900 tỷ đồng, tương đương 642 triệu USD, nhiều hơn 21% so với mức thiệt hại của năm 2017.

Ngày 4/6/2019, đại diện Đại học Quốc gia Australia cho biết trang mạng của trường đã bị tấn công quy mô lớn nhằm đánh cắp những dữ liệu nhạy cảm được lưu giữ trong vòng 19 năm qua. Phó hiệu trưởng Brian Schmidt cho biết các dữ liệu bị đánh cắp gồm tên, địa chỉ, ngày sinh, số điện thoại, địa chỉ hòm thư điện tử và các thông tin liên lạc trong trường hợp khẩn cấp, mã số hồ sơ thuế, thông tin đóng học phí, thông tin tài khoản ngân hàng và hộ chiếu. Tin tặc cũng đã tiếp cận được thông tin điểm học của sinh viên.[5]

Các trường đại học không có lựa chọn nào khác ngoài việc chú ý đến các mối đe dọa hiện nay và đảm bảo các biện pháp an ninh cần thiết để bảo vệ thông tin trước tội phạm mạng.

2. Lý do tấn công web server

Tin tặc có rất nhiều lý do để tấn công tất cả các trang web trên internet. Khi tấn công được một website, chúng có thể:

- Biết được thông tin quan trọng trong cơ sở dữ liệu (thông tin thẻ tín dụng, thông tin khách hàng,...).
- Điều hướng người truy cập tới trang lừa đảo (phishing)
- Lợi dụng tài nguyên (băng thông) của hệ thống để sử dụng bất hợp pháp, đặt quảng cáo trên web.
- Bán thông tin người dùng
- Sử dụng website như một công cụ để trục lợi trong SEO: kéo lưu lượng, điều hướng truy cập về web khác, v.v...

Tin tặc sử dụng các công cụ có thể "quét" tất cả các website trên internet, từ đó tìm ra các website có bảo mật yếu để tấn công.

Bằng chứng là vụ bắt giữ hồi cuối tháng 5/2019 đối với 4 đối tượng "Hacker sinh viên" tại đại học Thái Nguyên - nhóm này đã thực hiện quét lỗ hổng của hàng trăm website ngân hàng và trung gian thanh toán - sau đó xâm nhập vào các tài khoản và chiếm đoạt số tiền lên tới 3 tỷ đồng.

3. Những tác hại khi server bị tấn công

Dữ liệu bị mất hoặc bị đánh cắp

Máy chủ web (Web Server) và máy chủ đào tạo (Web edu) có chứa những dữ liệu quan trọng cần thiết như dữ liệu của nhà trường và dữ liệu đào tạo. Bao gồm: thông tin về nhà trường, các hoạt động, thông tin cá nhân và thông tin về điểm của sinh viên hàng chục ngành sinh viên các khóa. Việc server bị tấn công sẽ ảnh hưởng nhiều đến các dữ liệu này: bị rò rỉ trên mạng, bị mất, bị hỏng hoặc bị xâm phạm, điều này có thể khiến các công việc trên server phải ngừng hoạt động. Và nhà trường có thể sẽ phải trả cái giá rất đắt khi dữ liệu quản lý điểm của sinh viên bị hỏng hoặc mất.

Để có thể khôi phục hoàn toàn và kịp thời dữ liệu, hãy lưu trữ dữ liệu đó ở một vài nơi. Sử dụng

nhiều hơn một nhà cung cấp dịch vụ lưu trữ cloud và dịch vụ sao lưu hàng ngày, cũng như sử dụng các dịch vụ khôi phục dữ liệu.

Google Blacklist

Google đang cố gắng làm cho Internet trở thành một nơi an toàn đối với mọi người. Khi các bot tìm kiếm của Google tìm thấy một số mã độc hại trong web của trường, Google sẽ gắn nhãn "Website may be hacked" hoặc đưa ra cảnh báo "Trang web này có thể bị tấn công" hoặc "Trang web này có thể gây hại cho máy tính của bạn" ngay bên dưới tên web để ngăn cản người dùng truy cập các vào web. Để được gỡ bỏ nhãn website bị tấn công và xóa web khỏi danh sách đen của Google cần phải đợi một hoặc hai tuần sau khi web đã được khắc phục.

4. Dấu hiệu nhận biết website bị tấn công

Dưới đây là một vài dấu hiệu cho thấy website đã bị xâm phạm:

- Giao diện trang chủ bị thay đổi, đôi khi hacker để lại lời nhắn.
- Trình duyệt (Chrome, firefox...) cảnh báo Virus khi truy cập vào website
- Web tự động đăng bài lạ, hoặc xuất hiện code/ script lạ trong mã nguồn.
- Khi truy cập vào website, người dùng bị tự động chuyển hướng sang các trang web lừa đảo...

5. Các phương pháp bảo mật cho máy chủ server

Máy chủ là một loại máy tính chuyên dụng, được thiết kế đặc biệt hơn hẳn các máy tính thông thường để có thể hoạt động 24/7/365 ổn định với tốc độ xử lý cao. Máy chủ (server) thường được đặt tại các phòng chất lượng, có điều kiện bảo quản đặc biệt như nhiệt độ thấp, hệ thống làm mát và nguồn điện ổn định,... để cung cấp dịch vụ cho nhiều máy tính khác trong hệ thống mạng internet hoặc mạng LAN. Trong một hệ thống, máy chủ có thể cung cấp dịch vụ đến hàng triệu máy khách theo các mô hình mạng cụ thể.

Nhiệm vụ chính của máy chủ là lưu trữ dữ liệu, cung cấp và xử lý dữ liệu rồi chuyển chúng đến các máy trạm (client) trong hệ thống trong thời gian ngắn nhất có thể. Vì vậy, máy chủ luôn trong tình trạng sẵn sàng, đợi client gửi yêu cầu để xử lý, chúng chỉ bị tắt đi khi gặp sự cố cần được bảo trì.

Server là nơi lưu trữ toàn bộ thông tin dữ liệu cá nhân của sinh viên, cán bộ công nhân viên trong trường cũng như quản lý và vận hành các phần mềm của nhà trường. Đó cũng là mục tiêu các hacker luôn hướng đến. Vì vậy, việc bảo mật dữ liệu cho máy chủ server là việc làm thường xuyên và cần thiết.

Một số phương pháp bảo mật trên SERVER/VPS WINDOWS

5.1. Đặt mật khẩu có độ phức tạp cao

Hiện nay, lỗ hổng bảo mật mà các hacker thường khai thác nhất không phải là những vấn đề kỹ thuật sâu xa mà chính là sự lỏng lẻo, thiếu cẩn trọng trong việc đặt mật khẩu của người quản lý tài khoản đó. Vì thế phải tạo các mật khẩu đủ mạnh có độ phức tạp cao hội tụ đủ các yếu tố sau:

· Mật khẩu mang tính ngẫu nhiên, không có nghĩa.

· Mật khẩu không có bất kỳ liên hệ nào với thông tin cá nhân của người dùng.

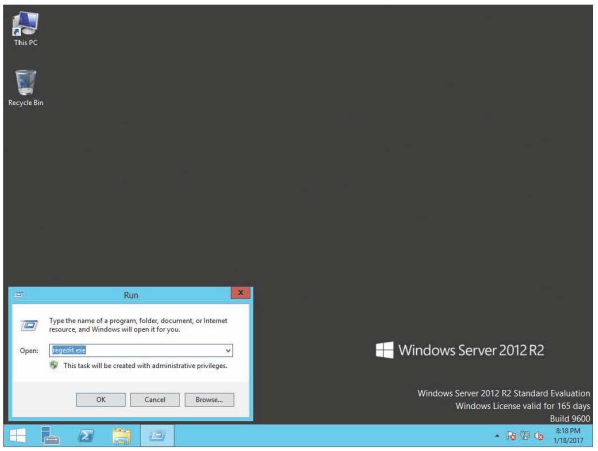
· Mật khẩu là tập hợp xen kẽ các ký tự số, chữ thường, chữ in hoa và ký tự đặc biệt.

Một số ví dụ về tài khoản có độ phức tạp và tính bảo mật cao: *B@oPnlM#1digsEJO, cD#Zd$FuwY23...*

5.2. Bảo mật remote desktop

Remote desktop là một tính năng trên các hệ điều hành Windows cho phép người dùng có thể truy cập và điều khiển hệ thống từ xa thông qua internet hoặc mạng nội bộ. Port mặc định của remote desktop là 3389, có thể thay đổi port mặc định này theo các bước sau:

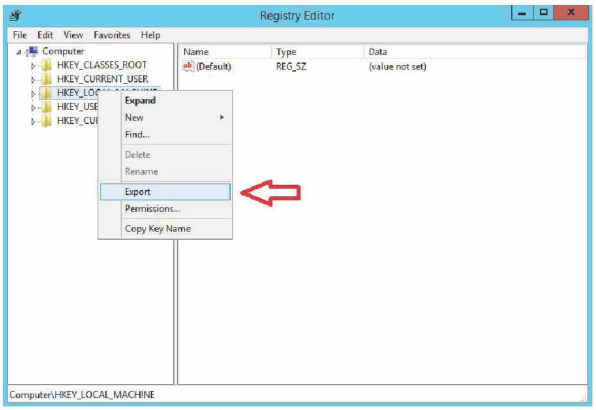
· Mở cửa sổ Registry Editor bằng cách bấm nút Start => Run (hoặc dùng tổ hợp phím Windows + R) => nhập regedit.exe



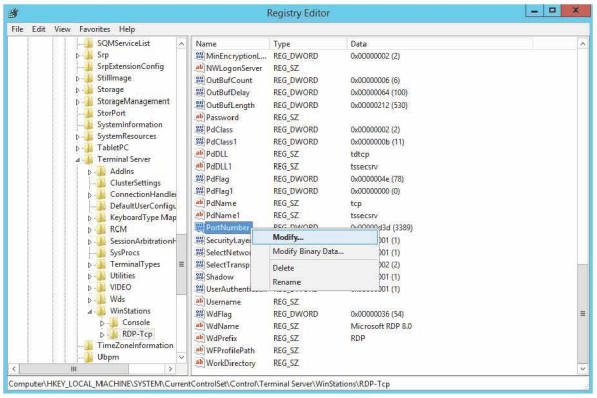
· Trước khi thực hiện chỉnh sửa bất kì registry nào, nên lưu lại một bản dự phòng của registry đó để tránh việc cấu hình sai làm ảnh hưởng tới hệ thống. Thực hiện: bấm chuột phải vào registry cần backup, chọn Export, chọn nơi sẽ lưu trữ bản dự phòng.

· Để thay đổi port hoạt động của remote desktop, truy cập đường dẫn sau trên Registry Editor:

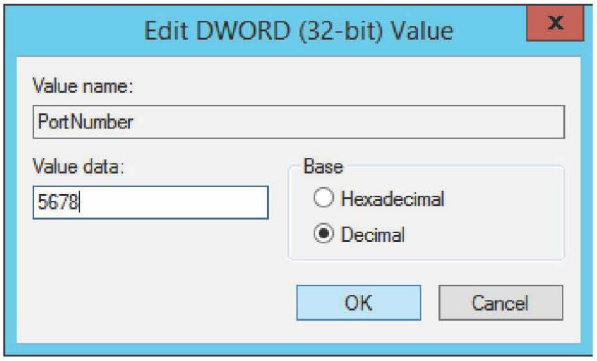
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber



· Nhấp chuột phải vào PortNumber, chọn Modify...



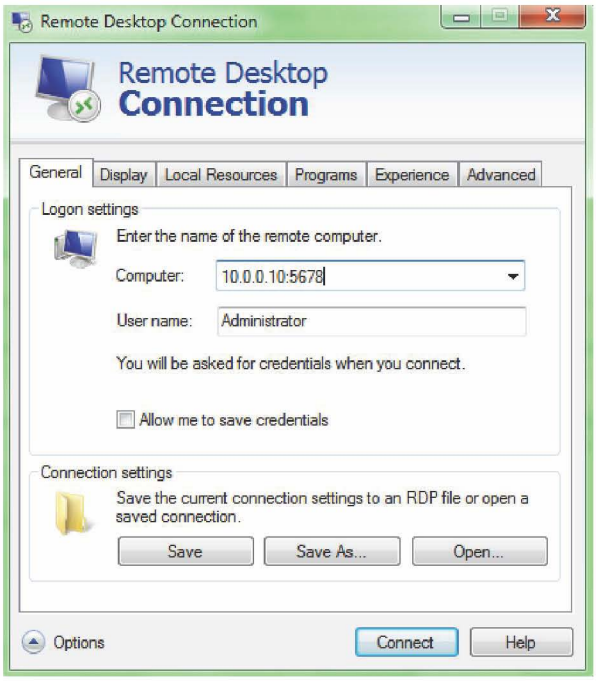
· Tại cửa sổ Edit DWORD, chọn Decimal để sử dụng hệ số thập phân, và thay đổi port hoạt động tại ô Value data, bấm OK



· Để truy cập và điều khiển máy tính từ xa, truy cập với địa chỉ <hostname>:<port> hoặc <địa chỉ IP>:<port>

5.3. Chặn các IP Quốc tế

Phần lớn các cuộc tấn công DoS/DDoS được ghi nhận thường bắt nguồn từ các IP nước ngoài. Để hạn chế cũng như ngăn chặn tình trạng này, người quản trị có thể chủ động cấu hình Windows firewall chặn các dãy IP quốc tế từng thực hiện tấn công



hoặc dải IP không mong muốn truy cập vào Server/VPS Windows bằng cách sau:

· Tải file script PowerShell tại đường dẫn sau và giải nén: https://live.vinahost.vn/img/232/import_firewall_blocklist.zip

· Mở cửa sổ Windows PowerShell với quyền Administrator bằng cách bấm nút Start, tìm từ khóa Windows PowerShell, bấm chuột phải vào kết quả tìm được và chọn Run as Administrator.

· Thực hiện lần lượt các lệnh sau:

PowerShell.exe -ExecutionPolicy Bypass

=> Cấu hình policy cho phép thực thi file script PowerShell.

cd Desktop

=> Di chuyển tới thư mục chứa file script (ví dụ đang đặt tại Desktop).

.\Import-Firewall-Blocklist.ps1 -zone CN

=> Thực hiện script, trong đó CN là mã quốc gia muốn chặn

Có thể tra cứu mã quốc gia 2 kí tự tại đường dẫn:

http://www.worldatlas.com/aatlas/ctycodes.htm

Có thể thực hiện chặn IP của nhiều quốc gia khác nhau bằng cách thực thi lại lệnh trên và thay thế mã quốc gia muốn chặn.

PowerShell.exe -ExecutionPolicy Restricted

=> Cấu hình lại policy thực thi file script PowerShell.

5.4. Vô hiệu hóa giao thức SMB

SMB (Server Message Block) là một giao thức

trên Windows cho phép người dùng chia sẻ tập tin, máy in, serial port... giữa các máy. Trong quá khứ, không ít các trường hợp kẻ xấu đã lợi dụng giao thức này để thực hiện tấn công các máy khác, và gần đây nhất là sự kiện WannaCry xảy ra vào tháng 5 vừa qua[8].

Để đề phòng việc bị kẻ xấu khai thác lỗ hổng bảo mật thông qua giao thức SMB, có thể chủ động tắt giao thức này trên Server/VPS bằng cách sau:

- Vô hiệu hóa SMB server
- Mở cửa sổ Windows PowerShell với quyền Administrator bằng cách bấm nút Start, tìm từ khóa Windows PowerShell, nhấp chuột phải vào kết quả tìm được và chọn Run as Administrator.
- Thực thi các lệnh sau:

>>> Đối với Windows server 2012:

Set-SmbServerConfiguration-EnableSMB1 Protocol $false

Set-SmbServerConfiguration-EnableSMB2 Protocol $false

>>> Đối với Windows server 2008:

Set-ItemProperty -Path "HKLM:\SYSTEM\ Current ControlSet\Services\LanmanServer\ Parameters" SMB1 -Type DWORD -Value 0 -Force

Set-ItemProperty -Path "HKLM:\SYSTEM\ Current ControlSet\Services\LanmanServer\ Parameters" SMB2 -Type DWORD -Value 0 -Force

- Khởi động lại Server/VPS
- Vô hiệu hóa SMB client
- Mở cửa sổ Command Prompt với quyền Administrator bằng cách bấm nút Start, tìm từ khóa Command Prompt, nhấp chuột phải vào kết quả tìm được và chọn Run as Administrator.
- Thực thi các lệnh sau:

sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi

sc.exe config mrxsmb10 start= disabled

sc.exe config lanmanworkstation depend= bowser/mrxsmb10/nsi

sc.exe config mrxsmb20 start= disabled

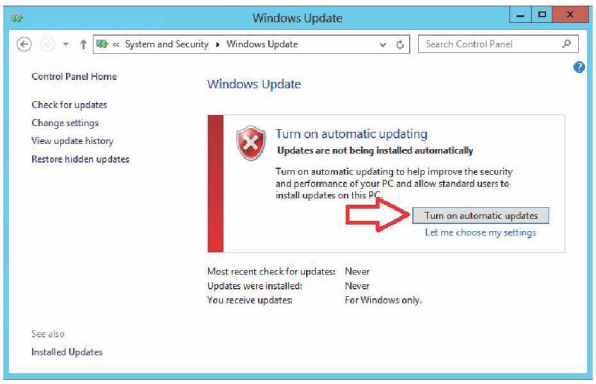
Khởi động lại Server/VPS

5.5. Cập nhật Windows

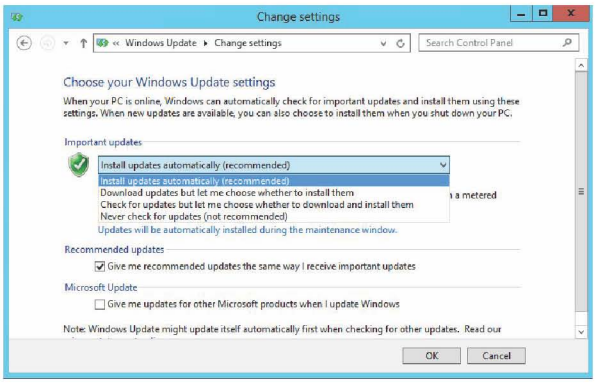
Một trong những biện pháp hữu hiệu nhất để phòng tránh việc bị kẻ xấu khai thác vào lổ hổng bảo mật là thực hiện cập nhật Windows thường xuyên. Có thể cấu hình cho Windows tự động cập nhật bằng cách sau:

· Truy cập Control Panel => System and Security => Windows Update

· Nếu Server/VPS chưa từng được cập nhật trước đây hoặc tính năng tự động cập nhật đang tắt, bấm vào nút Turn on automatic updates.



· Ngoài ra, có thể tự chọn kế hoạch thực hiện cập nhật Windows bằng cách chọn mục Change settings phía bên trái, sau đó chọn kế hoạch cập nhật mong muốn:



· Thông thường, sau khi cập nhật một số bản vá nhất định, Windows sẽ yêu cầu người dùng khởi động lại hệ thống để hoàn tất quá trình cài đặt. ❑

Tài liệu tham khảo

1. VMWare, Thách thức học đường: Tấn công mạng trong trường đại học, 2016.
2. Bộ Giáo dục Hoa Kỳ, Công cụ phân tích dữ liệu an toàn và bảo mật trong trường học, 2018.
3. HUB, Trường Đại học - Một mỏ vàng dữ liệu cá nhân cho tin tặc, 2017.
4. Tạp chí Campus Safety, Khảo sát quản lý ra vào trường học an toàn, 2017.
5. https://www.msn.com/vi-vn/news/world/tấn-công-mạng-quy-mô-lớn-nhắm-vào-trường-đại-học-hàng-đầu-australia/ar-AACmtGx
6. Tổng hợp từ Bản đồ tấn công website toàn cầu (01/01/19 - 30/06/19).
7. Báo cáo số 32/BC-CATTT, Tóm tắt tình hình an toàn thông tin đáng chú ý trong tuần 29/2018.
8. Abi Tyas Tunggal, What is the WannaCry Ramsomware Attack, 1/11/2019.