Bkav

NGHIÊN CỨU

22% WEBSITE TRÊN THẾ GIỚI tồn tại lỗ hổng

Tháng 3 - 2014

Mục lục

Giới thiệu

Trong những năm gần đây, các vụ tấn công xâm nhập website, các vụ lộ lọt thông tin xảy ra ngày càng nhiều, với hình thức tinh vi và mức độ ngày một nghiêm trọng hơn, gây thiệt hại hàng tỉ USD cho các công ty, tổ chức, và ảnh hưởng đến hàng triệu người dùng. Trong nhiều trường hợp, những vụ tấn công website không chỉ nhắm tới mục đích kinh tế mà còn bao hàm xung đột chính trị.

Cuối tháng 7 năm 2013, tòa án Mỹ đã khởi tố vụ án 160 triệu thẻ tín dụng bị ăn cắp bởi một nhóm hacker người Nga trong suốt 7 năm (2005-2012). Nhóm này đã thực hiện tấn công vào website của một số công ty lớn trong lĩnh vực bán lẻ và cung cấp dịch vụ tài chính như Nasdaq, Dow Jones, J.C. Penny, Visa Inc, chuỗi cửa hàng 7-Eleven, hệ thống thanh toán Heartland, các ngân hàng Bỉ - Dexia Bank, Carrefour SA (CA) - nhà bán lẻ lớn nhất của Pháp…

Đầu năm 2013, một báo cáo chi tiết của hãng bảo mật Mandiant - Mỹ đã chỉ ra dấu vết của các thành viên thuộc nhóm hacker Trung Quốc có liên quan tới một đơn vị quân đội của nước này. Nhóm hacker này đã lợi dụng lỗ hổng trên hệ thống để cài phần mềm gián điệp, theo dõi đánh cắp dữ liệu của các công ty, tổ chức lớn tại Mỹ trong nhiều năm.

Xa hơn, khoảng tháng 10 năm 2010, trang WikiLeaks công bố hàng trăm nghìn báo cáo chiến trường, video ghi lại cảnh tấn công bằng trực thăng của quân đội Mỹ trong đó có hình ảnh của những người dân vô tội bị giết hại... Sự cố lộ lọt thông tin tối mật lớn nhất trong lịch sử nước Mỹ này bắt đầu từ quân nhân Mỹ Bradley Manning. Nhiều chuyên gia cho rằng Bradley Manning có thể dễ dàng lấy những thông tin tối mật là vì các hệ thống chưa đủ an ninh.

Câu hỏi được đặt ra là: do đâu có sự lộ lọt của nhiều thông tin quan trọng từ những công ty, tổ chức tài chính được coi là phải có mức độ an ninh cao như thế? Tương tự như vậy, mỗi khi có xung đột giữa các quốc gia, các tổ chức chính trị, tại sao luôn xảy ra hàng loạt các cuộc tấn công chỉ sau 1 ngày? Các chuyên gia của Bkav nhận định: Nguyên nhân sâu xa có thể là sự tồn tại của lỗ hổng website. Đây là lý do để Bkav thực hiện nghiên cứu về thực trạng các lỗ hổng website hiện nay trên toàn cầu.

Phương pháp nghiên cứu

Một hệ thống quét website để tìm lỗ hổng đã được thiết lập để thực hiện nghiên cứu này. Trước khi quét, chúng tôi tập hợp danh sách website của các công ty, tổ chức tại nhiều quốc gia khác nhau trên thế giới. Tại mỗi quốc gia, khoảng 20 website của các công ty thuộc top đầu danh sách niêm yết trên thị trường chứng khoán được lựa chọn. Sở dĩ tiêu chí lựa chọn này được sử dụng vì chúng tôi tin rằng đây là website của các công ty lớn tại mỗi quốc gia nên sẽ được đầu tư và bảo vệ tốt nhất tại quốc gia đó, và website của các công ty, tổ chức khác mức độ an ninh sẽ còn kém hơn. Cuối cùng, chúng tôi đã chọn ra 516 website của các công ty tổ chức lớn tại 25 quốc gia đại diện cho các khu vực khác nhau trên thế giới như Mỹ, Anh, Hà Lan, New Zealand, Hàn Quốc, Nhật Bản, Mexico, Nam Phi... và Việt Nam. (Số liệu chi tiết về kết quả quét lỗ hổng website ở từng quốc gia có trong Phụ lục)

Thời gian thực hiện

Nghiên cứu này được thực hiện trong 7 tháng, từ tháng 7 năm 2013 đến tháng 2 năm 2014 với 4 lần quét trên hệ thống Bkav WebScan – Hệ thống kiểm tra và đánh giá lỗ hổng website.

Quá trình thực hiện

Từ tập mẫu là 516 website đã được lựa chọn, các chuyên gia Bkav tiến hành thêm địa chỉ của các website này lên cơ sở dữ liệu của hệ thống Bkav WebScan. Sau đó, chương trình kiểm thử được kích hoạt và tự động quét kiểm tra tìm kiếm lỗ hổng của lần lượt từng website. Với mỗi website, Bkav WebScan sẽ kiểm thử với nhiều loại lỗi khác nhau như: SQL Injection, Blind SQL Injection, XSS... Dựa trên các phản hồi từ các website, Bkav WebScan sẽ đánh giá các thành phần tồn tại lỗ hổng, kiểu lỗ hổng, mức độ nguy hiểm.

Khi quá trình kiểm thử này hoàn tất, kết quả quét được xuất ra file HTML. Kết quả sau đó được các chuyên gia Bkav phân tích, đánh giá.

Dựa vào kết quả quét, Bkav WebScan chỉ ra những vấn đề chính sau:

- Tổng số lỗ hổng tồn tại ở từng website
- Mức độ nguy hiểm của từng lỗ hổng tồn tại trên website
- Các loại lỗ hổng website có mức độ nguy hiểm cao như: SQL injection, XSS, Xpath injection...

Mô hình hoạt động của Bkav WebScan

Hệ thống Bkav WebScan kiểm tra lỗ hổng an ninh website theo hướng tiếp cận black box. Với hướng tiếp cận này, hệ thống sẽ gửi dữ liệu fuzz lên server chứa website hoặc truy cập thẳng vào đường link của website kèm theo dữ liệu gây lỗi, nhận dữ liệu từ website trả về và đưa vào bộ phân tích trước khi đưa ra kết luận về lỗ hổng.

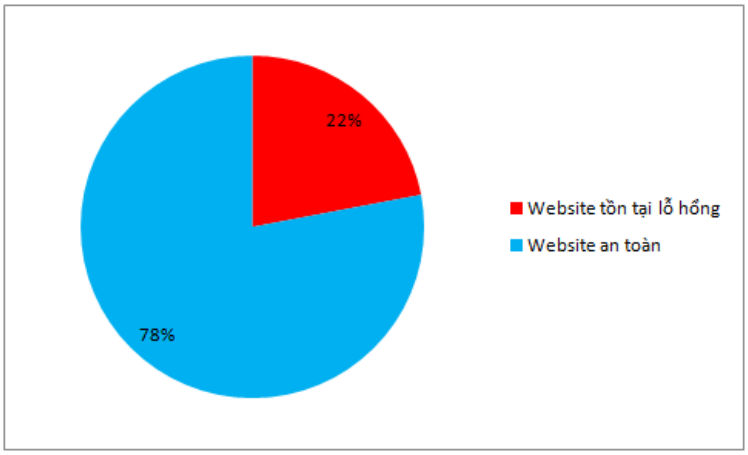
Dữ liệu fuzz là một tập hợp chứa dữ liệu nhận dạng, được kết hợp với một số thành phần của URL hoặc với những dữ liệu mà website xử lý. Dữ liệu fuzz sử dụng cho nghiên cứu này được chúng tôi tổng hợp từ kinh nghiệm thực tế kiểm tra lỗ hổng, vá lỗi website của

chính Bkav trong nhiều năm qua. Điều này đảm bảo tính chính xác cho việc nhận diện lỗ hổng của Bkav WebScan.

Với mỗi loại lỗ hổng, hệ thống kiểm thử dựa vào tập mẫu được xây dựng một cách tỉ mỉ từ kinh nghiệm của các chuyên gia của Bkav. Ví dụ, chỉ riêng tập mẫu nhận dạng lỗi XSS của Bkav WebScan đã có hơn 40 mẫu. Đối với một người chuyên lập trình web đơn thuần, việc xác thực dữ liệu đầu vào để tránh có lỗ hổng còn khá hạn chế vì đa phần họ chỉ chú ý vào việc tạo ra một trang web hoạt động "trơn tru" hơn là một hệ thống an toàn. Còn đối với một chuyên gia an ninh, việc xây dựng được một tập mẫu nhận diện đủ lớn để phòng tránh chỉ một lỗi như XSS với khoảng trên 40 mẫu thử là việc rất khó khăn và đòi hỏi nhiều năm tích lũy kinh nghiệm.

Các phát hiện chính

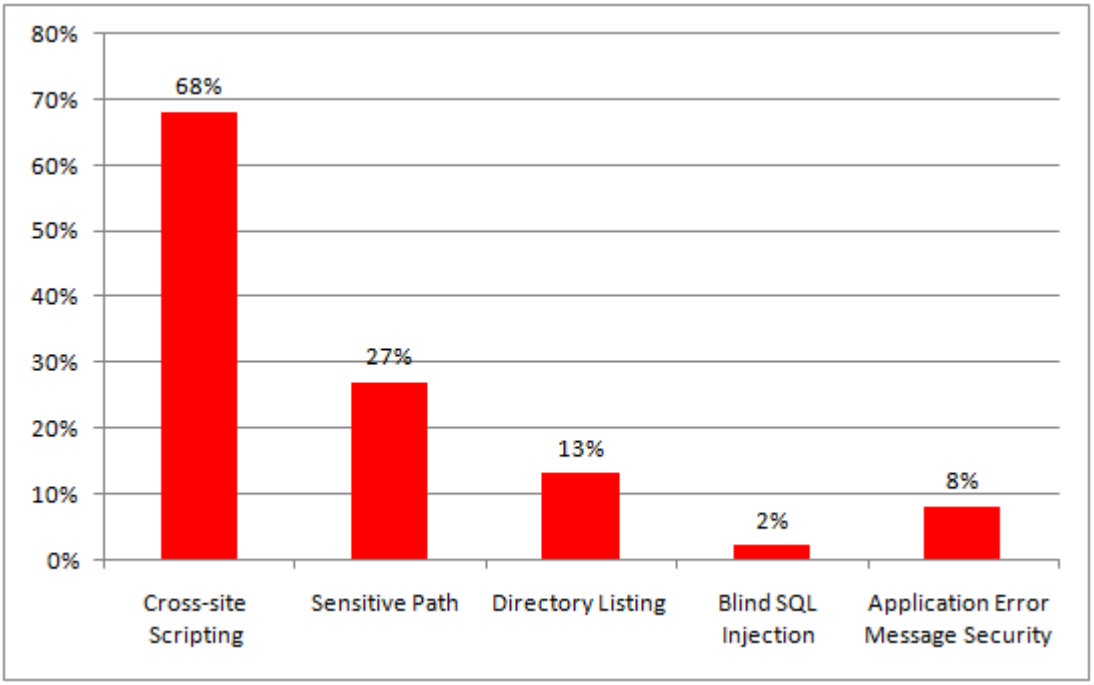
1. 22% website tồn tại lỗ hổng



114 trong tổng số 516 website được quét, tức là khoảng 22%, tồn tại lỗ hổng. Đây là tỉ lệ khá lớn, và thường nếu một website đã có lỗ hổng thì sẽ có nhiều lỗ hổng cùng tồn tại. Số lỗ hổng lớn nhất trên 1 website mà Bkav WebScan ghi nhận được là 407, và con số trung bình là từ 10 đến 20.

22% website tồn tại lỗ hổng là mảnh đất màu mỡ cho bất kì kẻ xấu nào với những kiến thức cơ bản về công nghệ cũng có thể dễ dàng lợi dụng để xâm nhập, tấn công vào hệ thống website của các cơ quan, tổ chức. Từ đó, chúng có thể tấn công leo thang đặc quyền để xâm nhập hệ thống, lấy cắp thông tin. Hơn thế, những người truy cập vào website đó cũng có thể trở thành nạn nhân, do một khi website đã bị tấn công cài đặt phần mềm độc hại thì hacker hoàn toàn có thể xâm nhập vào máy tính của người dùng. Cuối năm ngoái, báo điện tử New York Times bị tấn công DNS khiến người dùng không thể truy cập được trong nhiều giờ chính là minh chứng cho việc những vụ tấn công website ảnh hưởng trực tiếp không chỉ đến lợi ích của các công ty tổ chức vận hành website đó mà tác động cả đến người sử dụng, những người thường xuyên truy cập website.

2. Có 5 loại lỗ hổng chính



Có năm loại lỗ hổng chính tồn tại trên các website là: Cros-site Scripting, Sensitive Path, Directory Listing, Blind SQL Injection và Application Error Message Security. Kết quả có tới 78 website, chiếm tỉ lệ 68% các website có lỗ hổng được kiểm tra, xuất hiện lỗ hổng loại Cross-site Scripting. **Cross-site Scripting** (XSS) là một trong những lỗ hổng phổ biến nhất hiện nay. Bất kì một website nào cho phép người dùng đăng thông tin mà không có sự kiểm tra chặt chẽ các đoạn mã nguy hiểm thì đều có thể tiềm ẩn lỗi XSS. Đây là loại lỗ hổng cơ bản và phổ biến nhất mà các kĩ sư vẫn thường mắc phải trong quá trình lập trình website. Hacker có thể lợi dụng lỗ hổng này để chiếm quyền điều khiển website của các quản trị.

Đứng thứ 2 là lỗ hổng loại **Sensitive Path** xuất hiện trên 31 website, chiếm tỉ lệ 27%. Đây là lỗi để lộ các đường dẫn nhạy cảm. Lỗi này sẽ rất nguy hiểm nếu đường dẫn bị lộ là trang admin hoặc đường dẫn đến trang cấu hình. Tình huống nguy hiểm nhất là hacker có thể can thiệp vào cấu hình website hoặc đăng nhập vào trang quản trị.

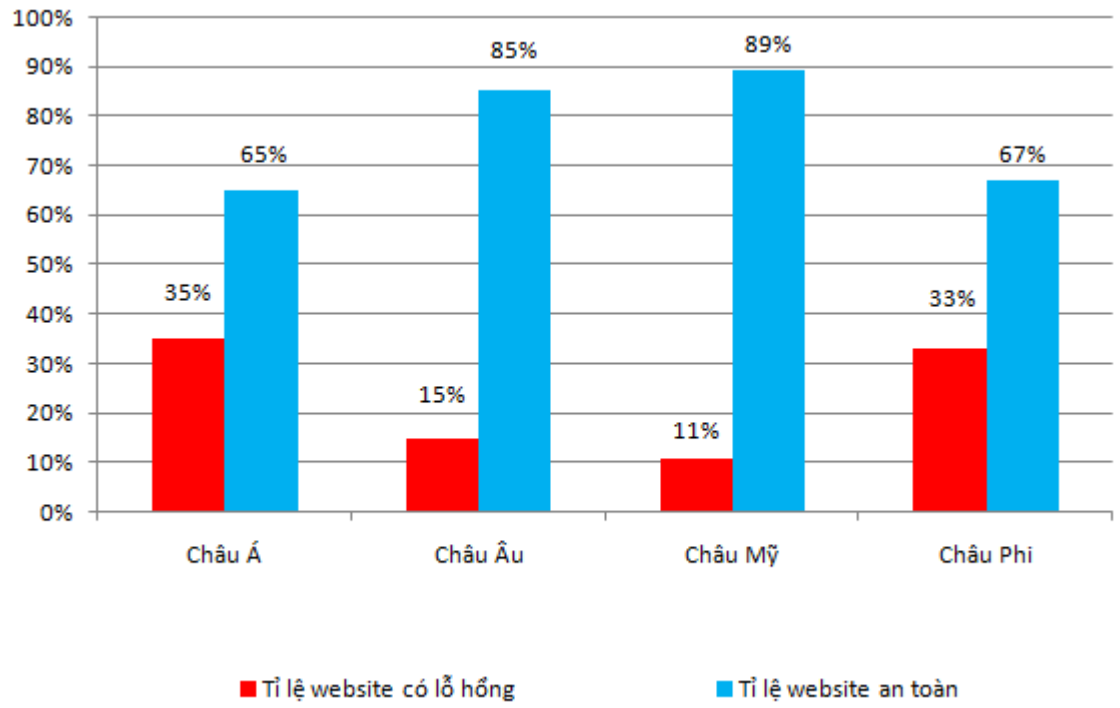
Directory Listing chiếm tỉ lệ 13%. Lỗ hổng Directory Listing xuất hiện nếu quản trị viên không cấu hình cho web server để ngăn chặn truy cập vào các danh sách thư mục. Khi một website bị mắc lỗi này, nếu người dùng truy cập vào một đường link thuộc website mà đó là một thư mục (*http://abc.com/folder/*), tất cả các tên file trong thư mục đó sẽ bị hiển thị trên trình duyệt người dùng. Directory Listing không quá nguy hiểm, nhưng sẽ gây hậu quả khó lường khi thư mục bị lộ có chứa các file bí mật mà quản trị không muốn người dùng bình thường nhìn thấy, chẳng hạn các file log, file cấu hình hoặc các file chứa những thông tin nhạy cảm.

8% lỗ hổng loại **Application Error Message Security** có nguyên nhân từ việc các thông báo của web server bị lộ trong quá trình lập trình hoặc gỡ lỗi. Application Error Message Security dù không gây nguy hiểm trực tiếp đến website, nhưng là bước đà để tìm ra và khai thác các lỗi khác nguy hiểm hơn.

Blind SQL Injection xuất hiện với tỉ lệ 2%. Kĩ sư khi lập trình website không kiểm tra các giá trị biến đầu vào khi đưa vào câu truy vấn cơ sở dữ liệu là nguyên nhân chính tạo nên lỗ hổng này. Hacker có thể lợi dụng để chèn thêm các câu lệnh không mong muốn, chiếm quyền điều khiển website, phá hoại cơ sở dữ liệu, lấy các thông tin bí mật như tài khoản tín dụng, tài khoản khách hàng… Dù chỉ xuất hiện ở một tỉ lệ nhỏ các website, Blind SQL Injection lại là mối đe dọa nguy hiểm nhất, trực tiếp nhất vì khai thác lỗ hổng này không cần qua các bước trung gian như các lỗ hổng khác.

Bkav nhận định đây là những loại lỗ hổng căn bản và phổ biến. Tuy nhiên mức độ nguy hiểm lại rất cao bởi kẻ xấu có thể dễ dàng tìm được những lỗi này nhờ vào công cụ thủ công, đơn giản hoặc thậm chí vô tình phát hiện ra. Nguyên nhân sâu xa có thể do kỹ năng lập trình an toàn của đội ngũ phát triển chưa cao cùng với việc rà soát, đánh giá kiểm tra chưa đúng theo quy trình. Hacker có thể lợi dụng lỗi sơ đẳng này để thực hiện hành vi tấn công gây ảnh hưởng trực tiếp đến website cũng như tác động đến hoạt động của công ty tổ chức cũng như những người sử dụng dịch vụ trên website của cơ quan, tổ chức đó.

3. Mức độ lỗ hổng tại các khu vực trên thế giới là khác nhau



Kết quả phân tích theo khu vực chỉ ra Châu Mỹ là khu vực có mức độ an toàn các website lớn nhất. Chỉ 11% số website tại khu vực này tồn tại lỗ hổng, 89% website đạt mức an toàn. Châu Âu và Châu Phi đứng thứ 2 và thứ 3 với chỉ số an ninh website ở mức 85% và 67%. Biểu đồ cũng chỉ ra Châu Á là khu vực có tỉ lệ website tồn tại lỗ hổng nhiều nhất, 35%. Kết quả này tương đồng với trình độ phát triển khoa học kĩ thuật và mức độ ứng dụng công nghệ thông tin của từng khu vực khác nhau trên thế giới.

Kết luận và Khuyến cáo

1. Kết luận

Kết quả trên không nằm ngoài dự đoán của các chuyên gia Bkav trước đó. Việc hơn 1/5 số website được quét tồn tại lỗ hổng, không còn nghi ngờ gì nữa, chính là nguyên nhân dẫn đến các thông tin về thẻ tín dụng, các thông tin kinh doanh, thông tin chính trị bí mật... bị lộ lọt. Đây là tiếng chuông báo động cho thực trạng an ninh an toàn hệ thống website trên toàn cầu. Các loại lỗ hổng website đa dạng với nhiều mức độ khác nhau chính là môi trường béo bở cho hacker dù chỉ với kiến thức cơ bản cũng có thể lợi dụng để xâm nhập tấn công gây hại cho hệ thống. Nguy cơ từ những lỗ hổng website không chỉ là vấn đề của riêng một cơ quan tổ chức nào mà đã trở thành mối nguy hiểm tại nhiều quốc gia, khu vực trên thế giới.

Từ kinh nghiệm nhiều năm trong lĩnh vực an ninh mạng, chúng tôi nhận định các lỗ hổng cơ bản của website xuất hiện là do hai nguyên nhân chính. Đầu tiên, các công ty, tổ chức chưa có quy trình kiểm tra đánh giá website định kì giúp phát hiện sớm những nguy cơ đang tồn tại trên website để có thể kịp thời đưa ra giải pháp bảo vệ. Đội ngũ lập trình website cũng chưa được trang bị kỹ năng lập trình an toàn là nguyên nhân thứ hai. Điều này dẫn đến những lỗi cơ bản trong quá trình code website, khiến cho website có lỗ hổng.

Không giống trong đời sống thực tế, con người có thể yên tâm vì đã được luật pháp bảo vệ. Trong thế giới mạng ngày nay, sự phát triển vượt bậc của công nghệ cũng đồng nghĩa với những mối nguy hiểm về an toàn, an ninh hệ thống không còn có biên giới. Hacker có thể ở quốc gia này nhưng thực hiện tấn công vào website của cơ quan, tổ chức tại các nước khác. Chính tốc độ phát triển như vũ bão của công nghệ làm vấn đề luật pháp dường như không thể theo kịp. Vì thế, các cuộc tấn công mạng, xâm nhập hệ thống đánh cắp thông tin xảy ra ngày một nhiều không chỉ hướng đến mục đích kinh tế mà còn bao hàm cả xung đột chính trị. Thực trạng này đòi hỏi cần có sự thay đổi về nhận thức từ các

chính phủ doanh nghiệp và thậm chí kiến thức của các kĩ sư lập trình cũng cần phải được thay đổi về căn bản.

Dựa vào tình hình thực tế qua quan sát, tổng hợp và phân tích cùng với hệ thống Bkav WebScan – Hệ thống kiểm tra và đánh giá lỗ hổng website, Bkav đã thực hiện nghiên cứu này giúp mọi người hiểu rõ hơn về hiện trạng an ninh của các website trên thế giới. Số liệu được hệ thống Bkav WebScan tự động ghi nhận, nên kết quả trên có thể chưa phải là tất cả. Trên thực tế con số có thể lớn hơn nhiều. Đây là nghiên cứu độc lập của Bkav, và những số liệu phân tích trong nghiên cứu không hướng tới việc đánh giá mức độ an ninh của bất kì một website thuộc cơ quan tổ chức nào.

Qua nghiên cứu này, các chuyên gia của Bkav cũng đưa ra khuyến cáo với mục đích giúp người quản trị website các cơ quan, doanh nghiệp có thể tăng cường mức độ an ninh thông tin của doanh nghiệp mình.

2. Khuyến cáo

Trong quá trình quản trị và vận hành hệ thống website, người quản trị nên có quy trình kiểm tra đánh giá website trước khi đưa vào sử dụng. Đồng thời, cần định kì kiểm tra để từ đó có biện pháp khắc phục các lỗ hổng, đảm bảo cho hệ thống website của mình được an toàn hơn. Thêm vào đó, các cơ quan tổ chức nên tiến hành đào tạo, củng cố, tăng cường kiến thức về lập trình an toàn. Khi tiến hành code website, các kĩ sư phải phân tích kĩ càng, lường trước được tất cả các tình huống có thể xảy ra để tránh "tạo" lỗ hổng website. Bkav cũng khuyến cáo các cơ quan doanh nghiệp nên sử dụng dịch vụ chuyên nghiệp được cung cấp bởi các công ty an ninh mạng để hệ thống website được an toàn nhất. Tại Bkav, chúng tôi luôn tổ chức đào tạo định kì cho đội ngũ kĩ sư, đồng thời có quy trình quét kiểm tra đánh giá lỗ hổng website định kì với Bkav WebScan cho hệ thống website nội bộ để đảm bảo an ninh thông tin được tốt nhất.

Về Bkav

Bkav là công ty hoạt động theo mô hình Tập đoàn công nghệ trong các lĩnh vực an ninh mạng, phần mềm, chính phủ điện tử, nhà sản xuất các thiết bị điện tử thông minh và cung cấp dịch vụ Cloud Computing. Công ty nằm trong Top 20 nhãn hiệu nổi tiếng nhất Việt Nam do Hội Sở hữu trí tuệ Việt Nam bình chọn.

Bkav là doanh nghiệp đầu tiên của Việt Nam lọt vào Danh sách các công ty hấp dẫn (Cool Vendors) tại các thị trường mới nổi trên toàn cầu do Gartner, Hãng tư vấn, nghiên cứu CNTT hàng đầu thế giới công bố. Công ty đã thành lập Bkav Singapore, và Bkav USA đặt tại Thung lũng Silicon, Mountain View, bang California – Mỹ.

Phụ lục

Dữ liệu thu thập qua Bkav WebScan

STT	Quốc gia *(sắp xếp theo bảng chữ cái)*	Số website có lỗ hổng	Số website an toàn
1.	***Cam-pu-chia***	9	12
2.	***Ấn Độ***	6	14
3.	***Anh***	3	21
4.	***Bỉ***	2	18
5.	***Bulgary***	4	16
6.	***Các Tiểu vương quốc Ả Rập Thống nhất***	5	17
7.	***Cộng hòa Czech***	2	18
8.	***Croatia***	3	17
9.	***Đài Loan***	4	15
10.	***Hà Lan***	5	15
11.	***Hàn Quốc***	8	12
12.	***Hungary***	4	16
13.	***Indonesia***	3	17
14.	***Malaysia***	8	12
15.	***Mexico***	1	19
16.	***Mỹ***	4	21
17.	***Nam Phi***	7	13
18.	***New Zealand***	2	18
19.	***Nhật Bản***	6	14
20.	***Pakistan***	4	19
21.	***Phần Lan***	3	17
22.	***Serbia***	8	13
23.	***Ukraine***	2	18
24.	***Venezuela***	5	15
25.	***Việt Nam***	6	15

Tham khảo

1. Emily Jane Fox, "CNN", <http://money.cnn.com/2013/07/25/pf/credit-card-hacking-scheme/index.html>, (25/8/2013)
2. Ryan W. Neal, "International Bussiness Time", <http://www.ibtimes.com/largest-financial-hack-ever-5-hackers-stole-160-million-credit-cards-hundreds-millions-dollars>, (26/8/2013)
3. Mandiant Report, <https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/> (20/3/2013)
4. Craig Lloyd, "Slashgear", <http://www.slashgear.com/anonymous-hackers-jailed-for-paypal-mastercard-visa-attacks-25266796/>, (30/8/2013)
5. Chris Plesance, "Dailymail" <http://www.dailymail.co.uk/news/article-2412465/Chelsea-Bradley-Manning-requests-Wikileaks-pardon-president-Barack-Obama.html> (5/9/2013)