THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 107 | Tháng 6 - 2020

MK group
Smart Digital Security

Tổng biên tập: *Bà Phan Thị Quỳnh Hoa - Giám đốc Tập đoàn MK* | **Ý kiến đóng góp vui lòng gửi về:** *marketing@mkgroup.com.vn*

Lưu ý: *Toàn bộ thông tin/hình ảnh trong Bản tin điện tử nội bộ Thế Giới Thẻ MK Group được sưu tầm từ các nguồn tin khác nhau và chỉ sử dụng cho mục đích chia sẻ kiến thức.*

CÁC TIN BÀI CHÍNH

LỄ BÀN GIAO PHẦN THƯỞNG ĐẶC BIỆT "BỐC THĂM MAY MẮN – QÙA TẶNG TỪ CHỦ TỊCH HĐQT"

Sáng 10/06, tại Nhà máy MK Smart đã diễn ra Lễ trao giải thưởng bốc thăm may mắn đặc biệt trong khuôn khổ hoạt động Lễ tổng kết hoạt động sản xuất kinh doanh năm 2019 – Định hướng phát triển của Tập đoàn MK trong năm 2020. Do ảnh hưởng từ các quy định liên quan tới giãn cách xã hội để ngăn chặn nguy cơ lây lan đại dịch COVID-19, hoạt động này đã phải dời sang đầu Quý II/2020. Mker may mắn là chị Nguyễn Thị Thúy Nga, nhân viên phòng Kiểm soát chất lượng (QC), với phần thưởng là một chiếc xe điện PEGA S trị giá 32.900.000đ.

Phần thưởng đặc biệt này là món quà bất ngờ được đích thân Chủ tịch Tập đoàn công bố và dành tặng cho một Mker may mắn, bên cạnh các quà tặng bốc thăm bằng hiện vật khác như tivi, lò nướng, lò vi sóng, nồi cơm điện và một số đồ gia dụng trong chương trình Bốc thăm may mắn trong Lễ tổng kết hoạt động sản xuất kinh doanh năm 2019.

Tham dự lễ trao giải thưởng có sự tham gia của ông Nguyễn Trọng Khang - Chủ tịch HĐQT MK Group, ông Đỗ Hải Đăng – Tổng Giám đốc MK Smart, ông Đoàn Linh – Chủ tịch HĐQT kiêm Tổng Giám đốc của PEGA cùng một số cán bộ nhân viên PEGA và MK Group.

PEGA, tiền thân là Hkbike, được biết đến là thương hiệu xe điện hàng đầu Việt Nam. Sau 5 năm gia nhập thị trường xe điện, đầu năm 2017, PEGA đã chính thức cho ra mắt những sản phẩm đầu tiên có tỷ lệ nội địa hoá tính theo giá trị sản phẩm lên đến 85%. Đây được xem là một bước đột phá quan trọng trong ngành sản xuất xe 2 bánh của nước nhà, khi mà lần đầu tiên có một sản phẩm xe 2 bánh được thiết kế bởi người Việt và được sản xuất tại Việt Nam. Phần thưởng xe máy PEGA S chính là sản phẩm mới nhất của hãng PEGA trong năm 2020 với những cải tiến vượt trội so với các sản phẩm cùng loại khác.

Hoạt động trao tặng giải thưởng bốc thăm may mắn với giá trị hiện vật không nhỏ như xe máy điện PEGA S minh chứng việc thực hiện cam kết của BLĐ MK cũng như thể hiện sự quan tâm và động viên kịp thời những nỗ lực lao động và cống hiến của các Mker trong quá trình gắn bó với MK Group. Đây cũng là hoạt động có ý nghĩa cổ vũ cho tinh thần ủng hộ các sản phẩm chất lượng cao của Việt Nam – " Make in Vietnam". Tương tự như sản phẩm thẻ của MK bao gồm thẻ tài chính giao diện kép theo chuẩn nội địa VCCS, thẻ EMV, thẻ sim Viễn thông, thẻ vé dành cho giao thông công cộng, thẻ ID, thẻ kiểm soát vào ra, thẻ thành viên ….

Chị Nguyễn Thị Thúy Nga, nhân viên QC - chủ nhân của phần thưởng đặc biệt, xúc động chia sẻ: "Tôi rất bất ngờ và rất vui vì đã được trở thành MKer may mắn của sự kiện. Từ sau Tết, tôi cũng rất háo hức chờ đón giải thưởng. Tuy nhiên, sau đó đại dịch CCOVID-19 bùng phát, doanh nghiệp nào cũng gặp khó khăn nhưng công ty vẫn thực chuẩn bị chu đáo và trao thưởng đúng như kế hoạch. Phần thưởng này sẽ giúp gia đình tôi đi lại và làm việc thuận lợi hơn. Xin cảm ơn Ban Lãnh đạo của MK rất nhiều."

Chương trình "Bốc thăm may mắn" trong Lễ tổng kết hoạt động sản xuất kinh oanh hàng năm của MK Group là hoạt động hết sức ý nghĩa được Ban Lãnh đạo tập đoàn cố gắng duy trì; bên cạnh nhiều việc làm đầy thiết thực và đáng trân trọng khác như Quỹ học bổng Khang & Friends do Chủ tịch Nguyễn Trọng Khang sáng lập với những khoản tiền hỗ trợ cho các gia đình CBNV và Mker nhí vượt qua hoàn cảnh để học tập tốt, lao động tốt.

Hy vọng những món quà đầy giá trị vật chất và tinh thần của Ban Lãnh đạo Tập đoàn sẽ góp phần giúp các CBNV của MK Group luôn yên tâm lao động, học tập và phát triển bản thân trong một môi trường làm việc chan chứa tình yêu thương, an toàn và tốt đẹp./.

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

Người Việt thích đi 'chợ mạng' sau dịch

Theo một khảo sát gần đây của Criteo về tác động của Covid-19 đối với hành vi tiêu dùng, 76% số người Việt được hỏi cho biết họ mua hàng trực tuyến nhiều hơn so với thông thường, trong khi chỉ có 15% mua sắm với tần suất tương đương.

Cũng theo khảo sát, những mặt hàng thiết yếu là lựa chọn chủ đạo. Cụ thể, 62% số người tham gia khảo sát nói họ mua hàng tạp phẩm và đồ dùng vệ sinh cá nhân qua giao dịch trực tuyến nhiều hơn.

Hệ thống dữ liệu thu thập được của Criteo cũng cho thấy, đầu năm đến nay, bán lẻ trực tuyến vẫn phát triển mạnh so với cùng kỳ năm 2019. Ông Steven Nguyễn, Giám đốc Cấp cao khu vực Đông Nam Á của Criteo chia sẻ, chung cả khu vực, có sự gia tăng của mua sắm trực tuyến, với nhiều sản phẩm khác nhau, từ chăm sóc sức khỏe sắc đẹp đến điện tử tiêu dùng, thực phẩm & đồ uống đến máy sinh trắc học.

"Các biện pháp như cách ly xã hội và hạn chế đi lại đã làm giảm mọi hoạt động và di chuyển. Vì thế, không thể tránh khỏi nhu cầu và thói quen hàng ngày của con người cũng thay đổi," ông Steven Nguyễn, đánh giá.

Trong một nhận định phát đi hôm 10/6, Visa Việt Nam cho rằng, sự chuyển dịch sang thương mại điện tử đang diễn ra ở phạm vi rộng hơn. Đồng thời, có sự biến chuyển trong chi tiêu đối với các sản phẩm thiết yếu hàng ngày như nhu yếu phẩm và dược phẩm.

Các chuyên gia trong ngành nhận định, cửa hàng trực tuyến hiện là đích đến của người tiêu dùng. Vì thế, nhà bán lẻ nên điều chỉnh trải nghiệm khách hàng hấp dẫn hơn, không chỉ thu hút khách trung thành mà còn những người mới./.

(VnExpress)

Nguồn: Internet

TIN VẮN THẺ NGÂN HÀNG

- **Nhằm hưởng ứng "Ngày không tiền mặt", từ ngày 16/06/2020 đến hết ngày 30/06/2020, Ngân hàng TMCP Ngoại Thương Việt Nam (Vietcombank)** phối hợp với Napas triển khai Chương trình ưu đãi với nhiều phần quà hấp dẫn dành cho các khách hàng giao dịch thành công bằng thẻ chip nội địa Vietcombank Connect 24.

- **Từ ngày 18/6 cho đến hết 30/6/2020, Ngân hàng Sài Gòn (SCB)** triển khai Chương trình ưu đãi " Ngày không tiền mặt cùng thẻ SCB NAPAS " dành cho tất cả các chủ thẻ chip nội địa SCB. Cụ thể, trong thời gian này khi các chủ thẻ chip nội địa SCB thực hiện các giao dịch thanh toán không dùng tiền mặt tại nhiều điểm bán hàng và trên các trang thương mại điện tử đều có cơ hội nhận được phần quà hấp dẫn như tiền mặt và vàng SJC 9999.

- **Từ ngày 1/6 đến 13/9/2020, Ngân hàng Đầu tư và Phát triển Việt Nam (BIDV)** triển khai chương trình khuyến mại chào hè với nhiều quà tặng hấp dẫn giá trị lên đến 100 triệu đồng cho các khách hàng phát hành mới thẻ ghi nợ nội địa, thẻ ghi nợ và tín dụng quốc tế nằm trong quy định./.

(Tổng hợp từ Internet)

Visa phát hành thẻ nhựa tái chế hoàn toàn

Visa đang lên kế hoạch phát hành các thẻ mới được làm từ nhựa tái chế cho tất cả các tổ chức tài chính trên toàn cầu.

Chương trình thẻ được hợp tác cùng với tổ chức Thẻ CPI nhằm tạo ra "Thẻ Trái Đất chất lượng cao" được làm bằng nhựa tái chế lên đến 98%. Dòng thẻ này có tích hợp EMV và giao diện kép có khả năng, cho phép thanh toán cả tiếp xúc và không tiếp xúc.

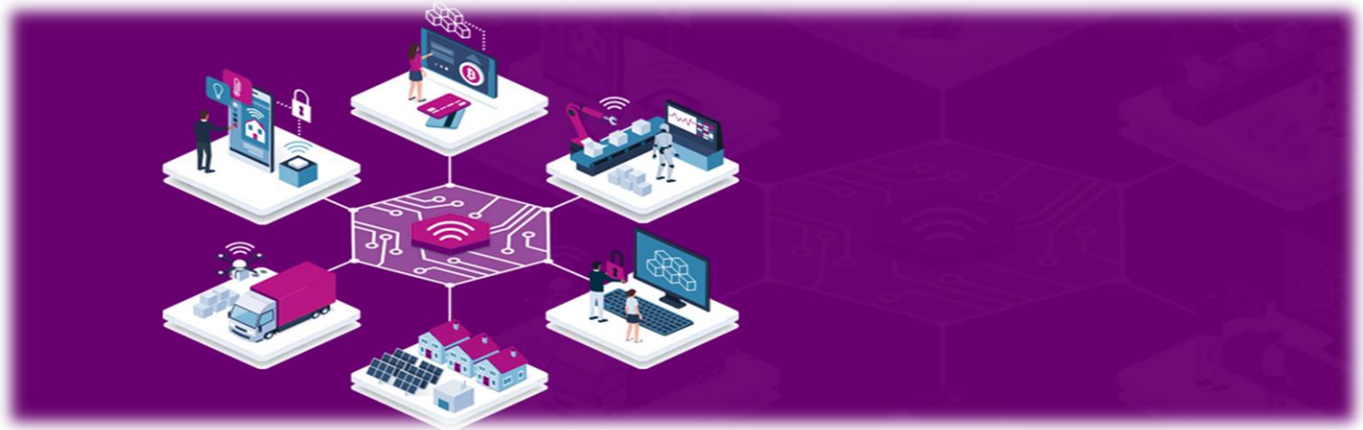
Douglas Sabo, phó chủ tịch quản lý chiến lược phát triển dài hạn của Visa cho biết "Sự hợp tác của chúng tôi với CPI biểu thị một cột mốc quan trọng hơn trong nỗ lực thúc đẩy mục tiêu tăng trưởng bao gồm với cam kết bảo vệ môi trường. Chúng tôi tin chắc rằng việc cung cấp này sẽ có lợi cho toàn bộ ngành công nghiệp thanh toán và môi trường."

Dòng thẻ mới này sẽ được xếp vào danh mục Earth Elements, các loại thẻ thanh toán thân thiện với môi trường của CPI, bao gồm Second Wave, một dòng thẻ thanh toán có lõi được làm bằng nhựa thu hồi từ đại dương./.

Nguồn: Internet

(Finextra)

ioTrust™ của Entrust Datacard®
đạt tiêu chuẩn ThingWorx Ready™



Entrust Datacard vừa gia nhập Mạng lưới Đối tác PTC, đồng thời tuyên bố nền tảng bảo mật Internet of Things (IoT) - ioTrust™ của hãng đã đạt được trạng thái ThingWorx Ready™.

Chương trình PTC ThingWorx Ready cho phép các công ty công nghệ xác nhận khả năng tương tác của các sản phẩm với nền tảng Industrial Internet of Things (IIoT) ThingWorx của PTC. Sau khi một sản phẩm được gắn mác ThingWorx Ready, sản phẩm đó sẽ xuất hiện trên không gian số PTC Marketplace, nơi các đối tác và khách hàng PTC có thể truy cập và quảng bá những công cụ IIoT, các giải pháp sẵn sàng cung cấp cho thị trường và những công nghệ tiên tiến được thiết kế để hỗ trợ các chương trình triển khai giải pháp.

Nền tảng ioTrust cung cấp các chứng chỉ số cho các thiết bị và cảm biến muốn kết nối an toàn với ThingWorx. Bằng cách quản lý chuỗi ủy thác và các cơ quan chứng nhận liên quan, các thiết bị và cảm biến sẽ nhận thông tin xác thực một cách an toàn từ ioTrust. Tất cả các thiết bị kết nối với ThingWorx có thể:

- Được xác thực bằng mật mã;
- Bảo mật dữ liệu thông qua TLS/SSL và mã hóa payload bằng cách sử dụng các API (Giao diện lập trình ứng dụng) Tác nhân Điểm cuối ioTrust để truy cập an toàn vào các thông tin đăng nhập được lưu trữ;
- Quản lý vòng đời của các chứng chỉ số một cách hoàn toàn tự động từ Bảng điều khiển quản lý dựa trên trình duyệt;
- Lưu trữ, khởi tạo và quản lý vòng đời của các khóa mã và chứng chỉ trên các điểm cuối và các ứng dụng Internet Vạn Vậtđược nhúng Tác nhân (Agent) IoT./.

(Entrust Datacard)

Quốc gia Châu Phi thử nghiệm thẻ sinh trắc học của Next Biometric

NEXT Biometrics và Softlock thông báo, thẻ thông minh sinh trắc học tích hợp giải pháp công nghệ chung đã được đưa vào giai đoạn thử nghiệm trong dự án chính phủ điện tử của một quốc gia châu Phi.

Thẻ thông minh sinh trắc học được trang bị cảm biến vân tay diện rộng, hết sức linh hoạt của NEXT và hệ điều hành của Softlock, cùng với cơ sở hạ tầng khóa công khai (PKI) và các ứng dụng sinh trắc học.

Loại thẻ thông minh trên sẽ được sử dụng cho xác thực bảo mật 2 yếu tố và đóng vai trò là nhân tố chính trong một sáng kiến nhằm mang lại cấp độ bảo mật cao hơn trong các dự án chính phủ điện tử. Sản phẩm chung của NEXT và Softlock sẽ thay thế các token PKI kèm mã PIN kém an toàn hơn bằng khả năng xác thực chính xác với vân tay của người dùng.

CEO của Softlock, ông Magdy Sharawy khẳng định: “Công nghệ cảm biến vân tay vượt trội và đã được chứng minh của NEXT bổ sung một cách lý tưởng cho các giải pháp bảo mật thông tin của chúng tôi. Trải nghiệm người dùng cuối liền mạch và trực quan là chìa khóa đối với sự chấp nhận và thành công của các giải pháp bảo mật.”

Sau giai đoạn thử nghiệm hiện tại, dự án thí điểm sẽ được triển khai ngay trong năm 2020./.

(Planet Biometrics)

Mastercard tiên phong cho phép đăng ký thẻ sinh trắc học từ xa

Mastercard vừa giới thiệu tiến bộ công nghệ mới dành cho thẻ sinh trắc học. Với công nghệ sinh trắc học đại diện cho thế hệ tiếp theo trong lĩnh vực bảo mật thanh toán, Mastercard đã phát triển một cách thức giúp người dùng có thể đăng ký vân tay trên thẻ sinh trắc học một cách dễ dàng và thuận tiện ngay tại nhà.

Mastercard đang thực hiện nhiệm vụ loại bỏ sử dụng mật khẩu và xác nhận người dùng thông qua yếu tố định danh, và thay vào đó bằng các công nghệ sinh trắc học như quét, nhận dạng khuôn mặt và quét mống mắt. Những tiến bộ trong công nghệ đang biến thanh toán sinh trắc học trở thành hiện thực, và thông qua hoạt động nghiên cứu và phát triển sâu rộng, công nghệ pin mang tính cách mạng giờ đây sẽ cho phép người dùng tự đăng ký thẻ sinh trắc học tiếp xúc hoặc không tiếp xúc. Vân tay của người dùng được quét bởi cảm biến trên thẻ và từ đó một bản mẫu kỹ thuật số mã hóa sẽ được tạo ra và lưu trữ an toàn.

Đơn giản hóa quy trình đăng ký sẽ giúp tăng tốc độ chấp nhận công nghệ sinh trắc học của các đơn vị phát hành và người tiêu dùng. Giải pháp mang lại hiệu quả về chi phí cho các đơn vị phát hành trong hoạt động cung cấp thẻ sinh trắc học quy mô lớn mà không yêu cầu cơ sở hạ tầng bổ sung tại các chi nhánh.

Với thẻ sinh trắc học, người tiêu dùng có được trải nghiệm an toàn mà họ yêu thích và có thể sử dụng tại mọi thiết bị đầu cuối EMV để thực hiện giao dịch thanh toán tiếp xúc hoặc không tiếp xúc. Đáng chú ý, các đơn vị phát hành còn được hưởng lợi từ sự nâng cấp khả năng phát hiện và ngăn chặn gian lận, gia tăng tỷ lệ chấp thuận và sự gắn bó của khách hàng. Đối với các đơn vị bán hàng, thẻ sinh trắc học tương thích với các thiết bị đầu cuối EMV hiện có nên sẽ không phải gánh thêm bất cứ khoản chi phí nào.

Năm 2017, Mastercard là tổ chức đầu tiên giới thiệu thẻ sinh trắc học kết hợp công nghệ chip với vân tay để xác minh bảo mật danh tính chủ thẻ cho các khoản thanh toán tại cửa hàng mà không cần tích hợp pin bên trong. Khi mua sắm và thanh toán tại cửa hàng, thẻ sinh trắc học hoạt động giống như bất cứ tấm thẻ nào khác tại các thiết bị đầu cuối EMV trên toàn cầu. Chủ thẻ đơn giản chỉ cần đặt ngón tay lên cảm biến được tích hợp trên thẻ và nhấn hoặc chạm vào tấm thẻ như bình thường. Với nguồn điện từ chính thiết bị đầu cuối, vân tay được xác minh bằng cách đối chiếu với mẫu đăng ký và - nếu trùng khớp - giao dịch có thể được chấp thuận sau đó, và tấm thẻ luôn nằm trong tay người tiêu dùng./.

(Mastercard)

FBI cảnh báo tấn công mã độc nhắm vào các ứng dụng ngân hàng đang gia tăng

Nguồn: Internet

FBI đã cảnh báo rằng tội phạm mạng và những kẻ lừa đảo đang tìm cách tấn công mã độc nhắm đến các ứng dụng Ngân hàng di động hòng đánh cắp thông tin đăng nhập người dùng và thực hiện các cuộc tấn công chiếm đoạt tài khoản.

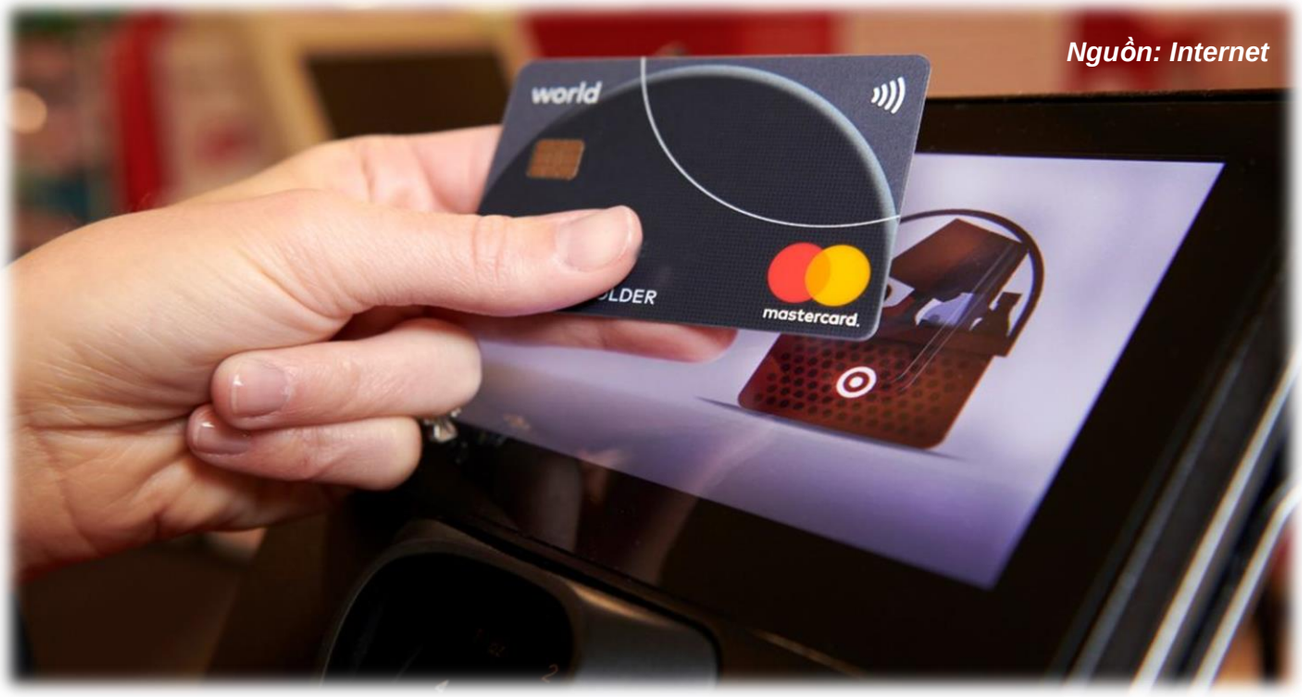
Trong cảnh báo mới được công bố mới đây, Trung tâm Tội phạm Internet của FBI đã đưa ra cảnh báo rằng những kẻ lừa đảo đang ngày càng nhắm đến tấn công độc hại ứng dụng di động vì đại dịch COVID-19 đã khiến ngày càng nhiều khách hàng chuyển sang sử dụng các ứng dụng Ngân hàng di động nhiều hơn.

FBI lưu ý "Người Mỹ đang ngày càng sử dụng nhiều hơn các ứng dụng Ngân hàng di động để thực hiện các tác vụ kiểm tra số dư tài khoản hay chuyển tiền. Và khi người tiêu dùng ngày càng sử dụng chúng nhiều hơn mỗi ngày vì phải hạn chế di chuyển bởi đại dịch, FBI dự đoán những kẻ tội phạm mạng sẽ sớm nhắm đến tấn công các nền tảng này."

Như một phần hệ quả của việc chuyển đổi này, những kẻ lừa đảo và tội phạm mạng đang tiến hành triển khai các phần mềm độc hại, như Trojans hay như thiết lập các ứng dụng giả mạo nhằm lừa đảo đánh cắp thông tin đăng nhập người dùng và thực hiện các cuộc tấn công chiếm đoạt tài khoản./.

(Govinfosecurity)

Thẻ thanh toán sinh trắc học dẫn đầu làn sóng không tiếp xúc



Nguồn: Internet

ABI Research dự báo, thẻ thanh toán sinh trắc học sẽ đóng vai trò chính trong xu hướng sử dụng các giao dịch thanh toán không tiếp xúc (TTKTX) đa nhân tố trong kỷ nguyên hậu COVID- 19.

Số lượng phát hành thẻ TTKTX dự kiến tăng thêm 110 triệu đơn vị so với dự báo trước đó - lên mức hơn 2 tỷ thẻ vào năm 2020, xuất phát từ nhu cầu về tương tác không chạm do đại dịch. Các con số mới này có nghĩa là lượng phát hành dự báo sẽ cao hơn khoảng 6% - 8% so với những ước tính trước đại dịch, tổng mức tăng trưởng hàng năm đạt 14%. Ước tính, 2/3 số thẻ mới phát hành trong năm nay sẽ là thẻ TTKTX.

Ông Phil Sealy, Giám đốc nghiên cứu của ABI Research nhận xét: “Mặc dù xu thế hướng tới TTKTX đã được hình thành rõ nét từ trước, song đại dịch COVID-19 sẽ khiến tốc độ chấp nhận TTKTX được đẩy mạnh hơn nữa, đặc biệt là ở các quốc gia và các nền kinh tế vốn ưa chuộng tiền mặt, đặc biệt, cả các nhân tố trong hệ sinh thái thanh toán cùng các chính phủ và tổ chức y tế như WHO đều khuyến khích sử dụng thẻ TTKTX ”.

ABI Research lưu ý, các tổ chức thanh toán lớn như Visa và Mastercard đã nâng hạn mức chi tiêu không tiếp xúc. Bên cạnh đó, một số cơ quan chính phủ đang hối thúc người dân hạn chế sử dụng tiền mặt, và thay thế bằng các phương thức thanh toán số./.

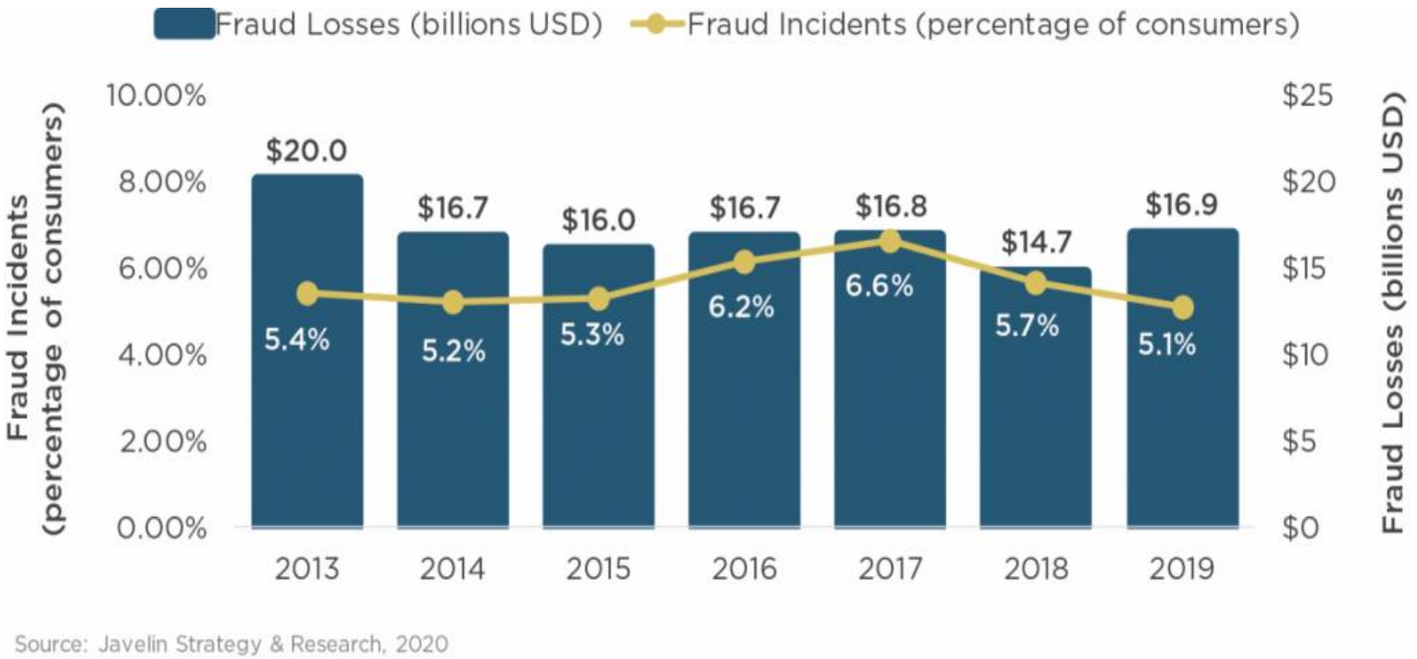
(Biometric Update)

Javenlin cảnh báo tình trạng gian lận chiếm đoạt tài khoản ở Mỹ

Báo cáo Gian lận Định danh năm 2020 cho thấy những phương pháp xác định và đối phó với gian lận của các tổ chức tài chính chưa theo kịp được các âm mưu tội phạm công nghệ cao nhằm chiếm đoạt tài khoản của người tiêu dùng.

Thiệt hại do gian lận đã tăng 15% trong năm 2019 lên mức 16,9 tỷ USD, bất chấp tổng số vụ việc đã giảm từ 14,4 triệu trong năm 2018 xuống 13 triệu vào năm 2019, khiến người tiêu dùng mất tới 3,5 triệu USD "bên ngoài ví" bởi giới tội phạm đã chuyển trọng tâm từ thẻ gian lận sang mở và chiếm đoạt các tài khoản.

Bà Krista Tedder - người đứng đầu bộ phận nghiên cứu gian lận của Javenlin Strategy & Research nhấn mạnh: "Những phát hiện này sẽ là một hồi chuông cảnh tỉnh dành cho các tổ chức tài chính, ngành thanh toán, các doanh nghiệp và người tiêu dùng trên khắp nước Mỹ… Dữ liệu là bằng chứng về những gì mà chúng ta đã biết lâu nay - toàn bộ mức độ nghiêm trọng của gian lận danh tính không chỉ nằm ở các loại thẻ tín dụng và thẻ từ giả mạo mà còn nằm trong hành vi chiếm đoạt toàn bộ tài khoản và gian lận tài khoản mới. Bây giờ chính là thời điểm để nâng cao hiểu biết của chúng ta về ý nghĩa thật sự của bảo mật, phát hiện và cách giải quyết".



Source: Javelin Strategy & Research, 2020

Nguồn: Internet

Nghiên cứu cho thấy các vụ chiếm đoạt tài khoản - là thủ đoạn đánh cắp thông tin định danh để truy cập trái phép vào tài khoản trực tuyến thuộc về người khác - đang có xu hướng gây ra nhiều thiệt hại nhất, gia tăng với tốc độ đáng kinh ngạc 72% so với 1 năm trước đó. Xu hướng này phần lớn dựa vào những thành tựu công nghệ giúp tội phạm dễ dàng thao túng và xử lý thông tin hơn, đồng thời khiến nỗ lực phát hiện các vụ chiếm đoạt tài khoản gặp thêm nhiều khó khăn nếu không có cơ sở hạ tầng bảo mật bổ sung. Giới tội phạm đang hành động một cách nhanh chóng - 40% trong tổng số hoạt động gian lận liên quan đến một vụ chiếm đoạt tài khoản xảy ra trong vòng 1 ngày.

Hình thức gian lận danh tính đã thay đổi mạnh từ làm giả thẻ tín dụng sang gian lận danh tính có tác động lớn đối với công tác kiểm tra và chiếm đoạt tài khoản tiết kiệm. Vào giai đoạn mà người tiêu dùng cảm thấy căng thẳng về tài chính do hậu quả của cuộc khủng hoảng y tế và kinh tế toàn cầu, tình trạng gian lận và lừa đảo chiếm đoạt tài khoản sẽ gia tăng. Vẫn còn quá sớm để dự đoán tỷ lệ gian lận sẽ tăng cao bao nhiêu, tuy vậy, giới tội phạm luôn hoạt động mạnh mẽ hơn trong những giai đoạn khó khăn về kinh tế.

Gian lận chiếm đoạt tài khoản là một trong những hình thức gian lận khó xác định nhất do truy cập tài khoản đa kênh và mong muốn nâng cao tính liền mạch trong trải nghiệm tiêu dùng. Công nghệ mới luôn sẵn sàng giúp giảm thiểu rủi ro và cải thiện trải nghiệm tiêu dùng, song nhân tố này thường không được sử dụng hoặc không có sẵn cho người tiêu dùng. Điều rõ ràng là giới tội phạm thích nghi với công nghệ mới nhanh hơn so với người tiêu dùng.

Nghiên cứu cũng chỉ ra rằng gian lận thanh toán ngang hàng (P2P), cho phép một người chuyển tiền cho một người khác, đang tăng vọt. Các tổ chức tài chính phát hiện thấy tình trạng gian lận tại các hệ thống P2P đã gia tăng tới 733% trong giai đoạn 2016 - 2019.

Thúc đẩy người tiêu dùng chuyển từ mật khẩu tĩnh sang sử dụng các phương pháp xác thực an toàn hơn là khuyến nghị dành cho các nhà cung cấp dịch vụ tài chính, các cửa hàng chấp nhận thanh toán và các công ty công nghệ khác. Dữ liệu cho thấy, người tiêu dùng sẵn sàng thực hiện sự thay đổi này, nhưng họ lại thiếu đi động lực.

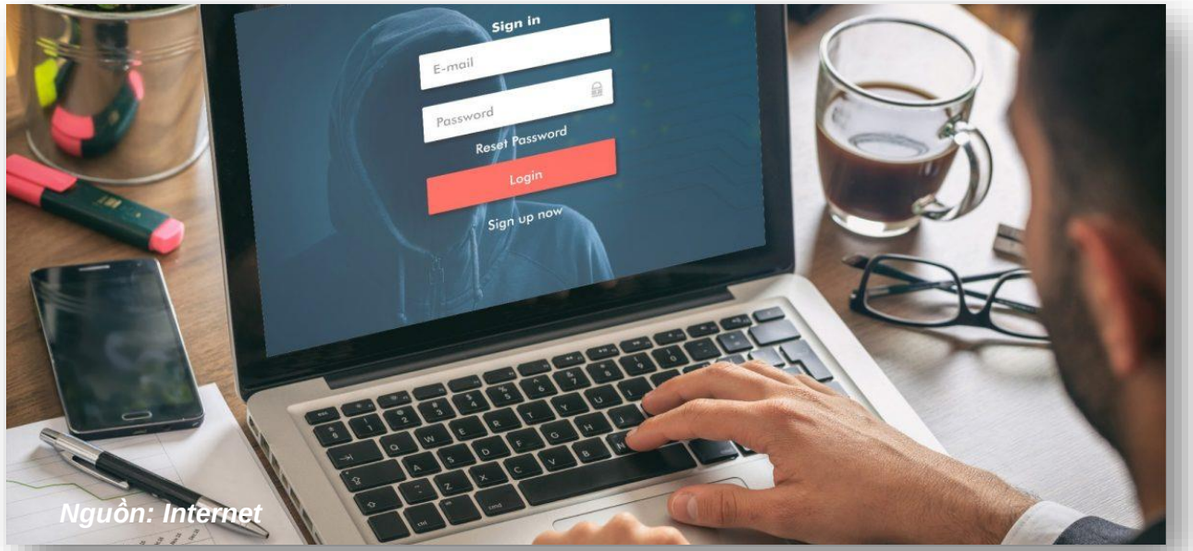
Những phát hiện mới nhất cũng chỉ ra sự cần thiết phải thay đổi rõ rệt trong cách thức mà các nhà cung cấp dịch vụ vụ tài chính, các cửa hàng thanh toán và các công ty công nghệ tham gia vào cuộc chiến phức tạp hơn bao giờ hết chống lại tình trạng gian lận.

Thực tế là: giới tội phạm thích nghi với công nghệ mới nhanh hơn so với người tiêu dùng, nên lĩnh vực dịch vụ tài chính phải chịu trách nhiệm dẫn dắt những thay đổi, chẳng hạn như gia tăng áp dụng công nghệ sử dụng xác thực 2 yếu tố và sinh trắc học, cũng như thúc đẩy ví kỹ thuật số nhằm làm giảm tác động nghiêm trọng của gian lận đối với xã hội./.

(Payments Cards and Mobile)

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

Tấn công bề mặt:
Phát hiện, ưu tiên và quản lý rủi ro (Phần cuối)



Nguồn: Internet

Làm cách nào để một tổ chức có thể bắt đầu khắc phục nguy cơ bị tấn công bề mặt? Làm cách nào mà một tổ chức có thể cắt giảm nhiều thành phần trong Sự hiện diện trên Internet - nhân tố gây ra những lỗ hổng trên thực tế. Trước tiên, tổ chức của bạn phải xác định tấn công bề mặt thực sự là gì.

Phát hiện và thiết lập sơ đồ về tấn công bề mặt

Bề mặt bị tấn công của một tổ chức chưa bao giờ được mở rộng như hiện nay. Các tổ chức hiện phải theo dõi nhiều loại tài sản xuyên suốt nhiều địa điểm khác nhau hơn bao giờ hết. Bất cứ chương trình phát hiện và thiết lập sơ đồ nào cũng nên khởi đầu bằng những yếu tố cơ bản như sau:

Những yêu cầu tổng thể:

- Bao phủ toàn bộ mạng Internet công cộng, trong đó có tất cả những nhà cung cấp dịch vụ đám mây lớn và không gian ISP thương mại (không chỉ trong những lĩnh vực đăng ký đã được biết đến);
- Lập danh mục toàn diện, mở rộng tất cả các cổng chính/cặp giao thức (thí dụ, không giới hạn trong quan điểm cũ về việc chỉ theo dõi các website HTTP và HTTPS);
- Tận dụng nhiều nguồn dữ liệu để phục vụ mục đích ủy quyền (chẳng hạn, không chỉ sử dụng bản ghi và dữ liệu DNS);
- Không phụ thuộc vào các đại lý (đơn vị không thể phát hiện những tài sản không được biết đến);
- Liên tục cập nhật (chẳng hạn với tần suất nhiều hơn 2 tuần/lượt).

Tầm quan trọng của phạm vi bao phủ toàn cầu đối với các tài sản

Trong quá khứ, phần lớn nguy cơ bị tấn công bề mặt đối với một tổ chức dựa trên những phạm vi "tĩnh" đã được biết đến. Ngày nay, các tổ chức cần phải tìm kiếm các tài sản của họ trong toàn bộ môi trường Internet.

Không gian IP trung tâm: Những phạm vi trung tâm là yêu cầu tối thiểu. Các tổ chức cần phải nhanh chóng giám sát các phạm vi đã được biết đến để phát hiện những điểm cấu hình sai hoặc các lỗ hổng thiết bị do sơ suất. Bất cứ sai sót nào trong các phạm vi này đều có thể bị phát hiện một cách nhanh chóng và ngay lập tức bị nhắm đến để phục vụ mục tiêu tấn công.

Những yếu tố phụ trợ và sáp nhập: Các đối tượng tấn công luôn tìm kiếm những điểm đột nhập ở bất cứ nơi nào mà chúng có thể, trong đó có những yếu tố phụ trợ được lồng vào nhau và các thương vụ sáp nhập trước đó. Expanse thường phát hiện các khoảng trống bị bỏ lại sau một thương vụ M&A (mua bán và sáp nhập) và không được giám sát. Các tổ chức nên chú ý tìm kiếm những tài sản bị bỏ quên trong quá khứ.

Các môi trường đám mây: Các tổ chức đang chuyển hướng hoạt động vào đám mây, và một nhân viên chưa bao giờ gặp nhiều thuận lợi như vậy khi tạo ra một thiết bị bên ngoài các quy trình CNTT thông thường. Các tổ chức nên tập trung vào việc phát hiện các tài sản bị nhắm đến trong mọi môi trường đám mây, trong đó có AWS, Azure, Google, Oracle, Rackspace, và những nhà cung cấp dịch vụ Cloud Hosting khác.

Không gian ISP thương mại: Lực lượng lao động di động đã tạo ra những rủi ro chưa từng tồn tại trước đây. Những nhân viên di động có thể cấu hình sai các trạm làm việc, qua đó khiến laptop của họ bị lộ ra trước toàn thế giới trên RDP (Giao thức Máy tính để bàn Từ xa). Những sơ suất này là hết sức nguy hiểm bởi chúng dịch chuyển khi nhân viên đó đi từ nhà tới một quán cà phê rồi tới một khách sạn.

Những nhà cung cấp chiến lược: Những nhà cung cấp hiện kết nối nhiều hơn bao giờ hết. Người ta thường không thể thực hiện công việc mà không chia sẻ các dữ liệu nhạy cảm hoặc cho phép các đối tác kinh doanh chủ chốt truy cập vào hệ thống. Những sơ hở trên các khu vực ven này trong hệ thống của bạn có thể dẫn đến tình trạng mất mát dữ liệu hoặc những hành vi đột nhập hệ thống vào doanh nghiệp của bạn.

Nhìn chung, những nhân tố khác nhau ở trên bổ sung vào toàn bộ mạng Internet toàn cầu. Các tổ chức hiện nắm trong tay những hệ thống "phủ sóng" rộng rãi đến mức họ cần phải giám sát toàn bộ mạng Internet để xác định một cách chính xác sự hiện diện trên Internet.

Các loại hình hệ thống kết nối

15 năm trước, sự hiện diện công khai trên Internet của phần lớn các tổ chức nằm ở những website. Ngày này, phần lớn các loại hình thiết bị khác bị bộc lộ đang khiến rủi ro trở nên nghiêm trọng hơn thông qua việc tạo ra những điểm vào trong một hệ thống.

Những kẻ tấn công liên tục tìm kiếm Telnet, SSH, SMB, và RDP, thậm chí nhiều hơn các website. Máy chủ cơ sở dữ liệu (CSDL) và các thiết bị hội nghị từ xa cũng là những mục tiêu phổ biến. Nếu bạn sơ hở trong bất cứ yếu tố vừa đề cập nào, một kẻ tấn công hầu như chắc chắn sẽ nhanh chóng phát hiện ra chúng.

Một số kỹ sư cho rằng, họ là người thông minh khi giấu các dịch vụ trên những cổng phi tiêu chuẩn, chẳng hạn như cổng 2323 dành cho Telnet, hoặc cổng 8000 dành cho HTTP. Dữ liệu của Expanse cho thấy, các đối tượng tấn công vẫn đang tìm kiếm những thiết bị trên các cổng thông dụng, phi tiêu chuẩn và cũng sẽ nhanh chóng phát hiện ra những tài sản đó.

Vấn đề tấn công bề mặt của bạn không chỉ bao gồm các máy chủ web, mà còn hàm chứa nhiều hình thức thiết bị khác như:

Cổng	Giao thức	Thiết bị thông dụng
80	HTTP	Máy chủ web
443	HTTPS	Máy chủ web
23	Telnet	Hạ tầng mạng
3389	RDP	Trạm làm việc, máy chủ
1433	SQL	Máy chủ CSDL

Giám sát tấn công bề mặt

Phát hiện và thiết lập sơ đồ tấn công bề mặt chỉ là bước đầu tiên. Công tác giám sát liên tục có vai trò hết sức quan trọng đối với nỗ lực duy trì sự an toàn. Những năng lực then chốt bao gồm:

- Giám sát liên tục;
- Triển khai những quy trình xoay quanh hoạt động cật nhật/thay đổi hệ thống của bạn, thí dụ như các nhà cung cấp dịch vụ đám mây mới, những phạm vi hệ thống mới;
- Thực hiện các hoạt động kiểm toán theo định kỳ;
- Giám sát toàn bộ vấn đề tấn công bề mặt để phát hiện ra những kết nối bất thường và rủi ro đến và đi từ hệ thống, thay vì chỉ giám sát các dịch vụ không được bảo vệ.

Thu hẹp bề mặt có khả năng bị tấn công

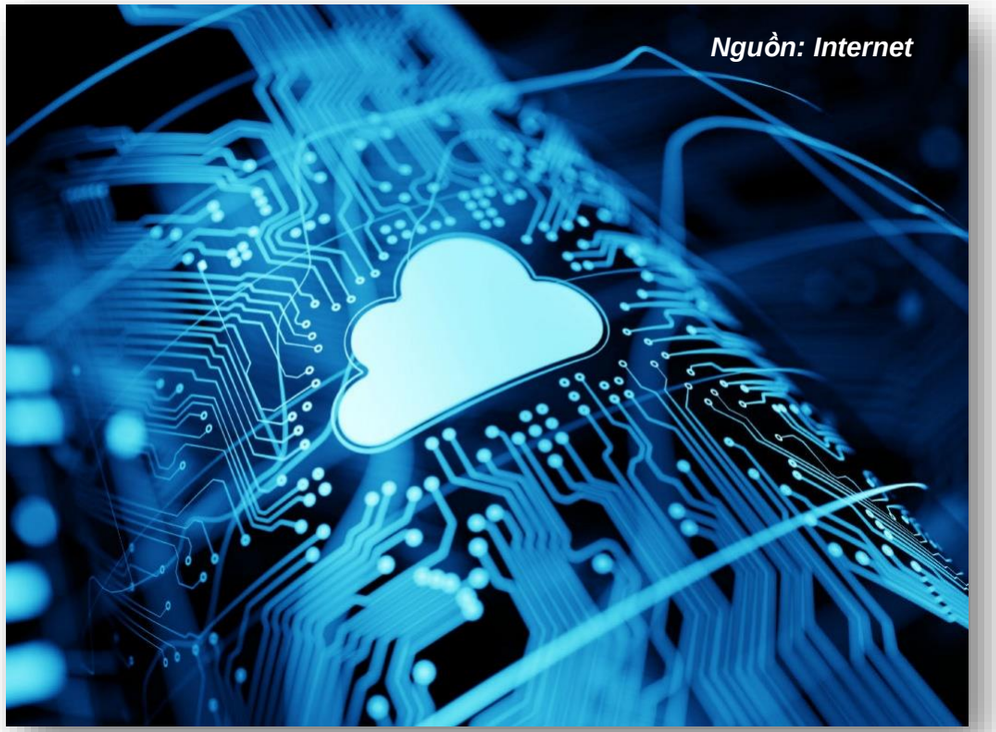
Khi bạn triển khai một chương trình toàn cầu và toàn diện phục vụ công tác phát hiện, giám sát và quản lý bề mặt có khả năng bị tấn công, bạn có thể tránh được một số rủi ro phổ biến nhất mà các tổ chức ngày nay phải đối mặt. Những rủi ro này bao gồm:

Mã độc tống tiền từ xa: Vấn đề RDP

RDP gần đây đã trở thành một điểm khởi đầu số 1 dành cho những cuộc tấn công bằng mã độc tống tiền (ransomeware). Một trạm làm việc bị lộ RDP trên mạng Internet công cộng chẳng khác gì với việc để mặc chiếc laptop hoạt động với màn hình đăng nhập trên đường phố, nơi bất cứ ai cũng có thể thử nhập username và password. Phần lớn các tổ chức cho rằng, họ đang khóa RDP trong toàn bộ mạng lưới và thiết bị, song Expanse thường phát hiện ra những thí dụ về RDP dành cho các tổ chức lớn trên mạng Internet công cộng, với phần lớn nằm trong danh sách Fortune 100.

Hoạt động tấn công phổ biến nhất nhằm vào RDP khởi đầu với một nỗ lực đoán mật khẩu kiểu “brute force” (kiểu tấn công được dùng cho tất cả các loại mã hóa. Brute Force hoạt động bằng cách thử tất cả các chuỗi mật khẩu có thể để tìm ra mật khẩu chính xác). Nếu mật khẩu không đủ độ khó hoặc nếu không có những nỗ lực “đóng cửa”, các đối tượng tấn công sau đó có thể thâm nhập vào một thiết bị. Một khi hành động này xảy ra, ransomware thường được cài vào, và có thể lây lan ra toàn bộ tổ chức, qua đó gây nên những sự cố gián đoạn hoạt động nghiêm trọng đối với doanh nghiệp. Dữ liệu có thể bị mã hóa hoặc hủy hoại, khiến một tổ chức đối mặt với một hệ thống bị tê liệt do một sơ suất không rõ xảy ra trên không gian IP mà họ không giám sát. Những sự sơ suất này cực kỳ khó để lần ra dấu vết bởi chúng thường xảy ra bên ngoài những địa điểm thường xuyên được đội ngũ CNTT và bảo mật của một tổ chức giám sát.

Bằng cách thiết lập danh mục mạng Internet toàn cầu nhiều lần mỗi ngày, Expanse giúp các khách hành phát hiện được những sơ hở như RDP trước khi họ bị nhắm đến.



(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

Các vấn đề đều nằm trong đám mây

Một số vụ rò rỉ dữ liệu trong năm 2018 không phải là những vụ hack điển hình, mà do một nhân viên gây nên, khi nhân viên này khởi chạy một máy chủ CSDL trong đám mây mà không thông báo với đội ngũ bảo mật. Các nhà phát triển thường sử dụng dữ liệu sản xuất để thay cho dữ liệu giả nhằm phục vụ công tác kiểm tra, và nếu những CSDL này tình cơ bị rò rỉ, việc "đánh hơi" ra chúng chỉ còn là vấn đề thời gian. Đội ngũ CNTT và bảo mật không được thông báo và không thể phát hiện ra chúng bởi vì những sơ hở này tồn tại ngoài chính sách.

Những sơ suất nói trên dễ xảy ra và có thể làm lộ lọt dữ liệu nhạy cảm cho các đối tượng xấu, mà chúng hầu như không cần đến bất cứ nỗ lực nào. Các tổ chức cần duy trì sự mẫn cán bằng cách tìm kiếm những lỗi cấu hình CSDL phổ biến (SQL, Elasticsearch, MongoDB, Memcached) không chỉ ở trên không gian IP, mà còn xuyên suốt toàn bộ các môi trường đám mây.

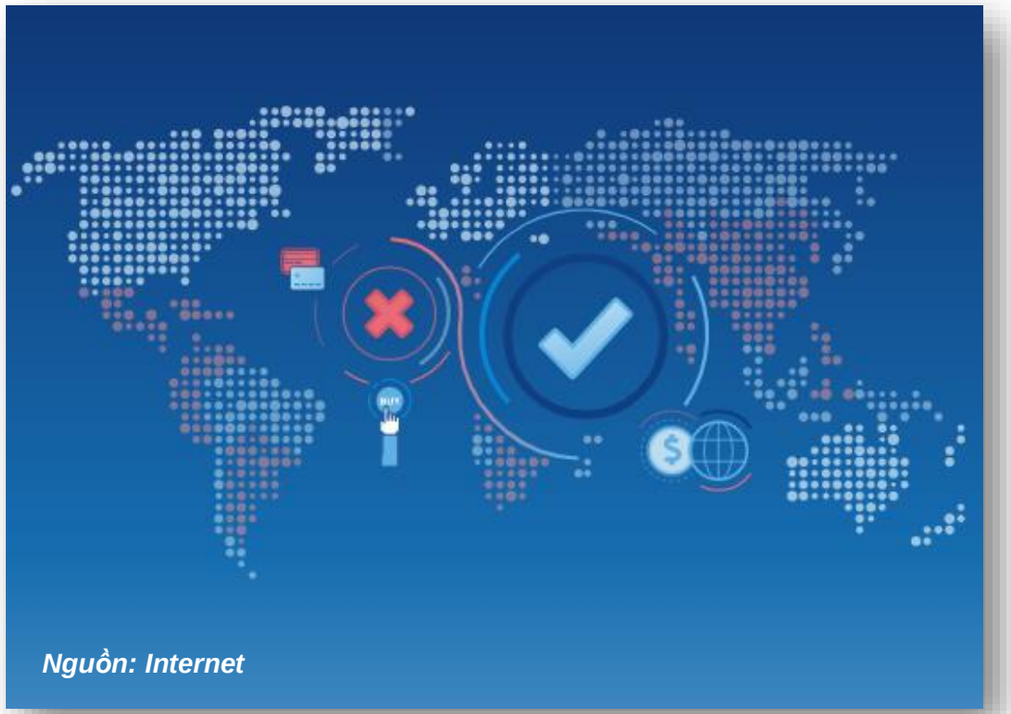
Không giao tiếp với "người lạ": Kiểm tra hoạt động thiết lập danh sách đen dựa trên GeoIP

Nhiều tổ chức cấm kết nối đến các quốc gia mà họ được khuyến cáo không nên thực hiện công việc kinh doanh. Về mặt pháp lý, các tổ chức tài chính bị ngăn cấm làm ăn với những quốc gia nhất định nằm trong bản danh sách của Văn phòng Kiểm soát Tài sản Nước ngoài (OFAC) thuộc Bộ Tài chính Mỹ. Những kết nối đến hoặc xuất phát từ Iran, Syria, hay Belarus không thể là lưu lượng hợp pháp. Phần lớn các tổ chức tài chính đã thiết lập danh sách đen nhằm ngăn chặn những sự kết nối với các quốc gia không được cho phép.

Đề nghị tham khảo: CSDL hành vi của Expanse bao gồm lưu lượng netflow được lấy mẫu trên toàn cầu. Netflow cơ bản là siêu dữ liệu về một kết nối. Bạn có thể thấy nguồn, Destination IP và cổng, nhưng bạn không thể thấy bất cứ thông tin nào về nội dung thực sự của tin nhắn. Những dữ liệu này độc lập và có phạm vi toàn cầu, mang lại một sự công nhận giá trị thật của dữ liệu nếu Geo-blocking được thực hiện một cách chính xác.

Expanse hầu như luôn tìm kiếm lưu lượng đến hoặc đi từ các quốc gia bị liệt vào danh sách đen, mặc dù phần lớn các tổ chức cho rằng họ đã thực hiện Geo-blocking. Thông qua hoạt động kiểm tra các luồng dữ liệu, đội ngũ bảo mật thường nhận ra rằng, họ chỉ có khả năng thấy được những kết nối Internet chính. Lưu lượng có thể bị rò rỉ ra khỏi hệ thống ở nhiều địa điểm khác, nơi đội ngũ an ninh không thể thấy được.

Bằng cách truy cập vào dữ liệu toàn cầu và độc lập, đội ngũ bảo mật không bị bó hẹp trong những gì mà họ biết. Thay vào đó, họ có thể thực sự thử nghiệm để phát hiện liệu chính sách Geo-blocking của mình có hoạt động thông qua công tác giám sát dữ liệu trên mạng Inernet toàn cầu hay không, thậm chí đối với nhiều khu vực trong hệ thống của họ - nơi họ không có bất cứ cảm biến lưu lượng địa phương nào.



Nguồn: Internet

Thay cho lời kết

15 năm trước, Internet từng là một không gian rộng lớn. Nếu bạn vô tình để lộ một thiết bị, nó có thể không bị phát hiện suốt nhiều tháng, hoặc thậm chí nhiều năm. Tuy nhiên, mọi việc hiện giờ đã khác. Những kẻ tấn công có thể "đánh hơi" được mọi thiết bị trên Internet trong vòng 45 phút. Bất cứ thao tác cấu hình sai hoặc sơ suất vô tình nào đều có thể bị phát hiện một cách nhanh chóng. Những cuộc tấn công trên phạm vi toàn cầu như WannaCry và NotPetya đã cho thấy cách thức mà một làn sóng tấn công mới không nhằm vào những doanh nghiệp cụ thể, mà tìm kiếm và tấn công vào những điểm yếu trên toàn cầu, bất kỳ ai sơ hở, ở bất kỳ đâu.

Tấn công bề mặt đã mở rộng để bao trùm lên đám mây, thậm chí là không gian ISP thương mại, từ đó gây ra những thách thức mới đối với các tổ chức đang cố gắng hạn chế những điểm vào trong các hệ thống của họ. Vì vậy, các tổ chức phải nỗ lực triển khai những giải pháp và công cụ cần thiết để phát hiện tấn công bề mặt và triển khai các biện pháp để thu hep tối đa bề mặt này, từ đó tạo ra một môi trường hoạt động an toàn hơn./.

(Expanse)

MK® group

Smart Digital Security

www.mkgroup.com.vn | contact@mkgroup.com.vn | www.facebook.com.vn/mkgroup1999

Hà Nội: Tầng 11, tòa nhà TTC, 19 Duy Tân, Cầu Giấy | Tel: (+84-24) 6266 2703

Tp. Hồ Chí Minh: Tầng 7 Thiên Sơn Building, 5 Nguyễn Gia Thiều, Quận 3 | Tel: (+84-28) 3930 5023