

THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 105 | Tháng 5 - 2020



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



- [MK Group – Vững vàng Tuổi 21](#)
- [Tỉ lệ sử dụng tiền mặt tại Việt Nam giảm do người tiêu dùng đón nhận những phương thức thanh toán mới](#)
- [Samsung hợp tác với SoFi phát hành thẻ ghi nợ](#)
- [Mastercard: Thanh toán không tiếp xúc tăng trưởng mạnh mẽ trên toàn cầu](#)
- [Tình trạng tấn công thiết bị đầu cuối gia tăng mạnh ở châu Âu trong năm 2019](#)
- [Tấn công bề mặt: Mỗi hiểm họa không thể xem nhẹ \(Phần 1\)](#)

MK Group – Vững vàng Tuổi 21

Tuổi 21 của MK Group diễn ra trong bối cảnh hết sức đặc biệt bởi những tác động tiêu cực trên toàn cầu của đại dịch Covid-19. Kể từ sau Thế Chiến II, đây chính là một trong những dịch bệnh có sức tàn phá nặng nề và phạm vi ảnh hưởng sâu rộng loài người phải đối mặt. Còn với riêng MK, điều này đúng với câu nói của người xưa: “Lửa thử vàng, gian nan thử sức”.

Quả thực, hành trình 21 năm của MK Group để hiện thực hóa khát vọng sáng tạo ra những sản phẩm, giải pháp công nghệ Việt mang hàm lượng chất xám cao, với nhiều lợi ích cho người Việt Nam không hề dễ dàng. Không chỉ phải đương đầu với những thách thức đến từ bên ngoài, MK còn phải đối mặt với chính những tồn tại đến từ bên trong doanh nghiệp. Không ngừng trên những thành công đã đạt được, các nhà lãnh đạo của MK thẳng thắn và dám nhìn vào những điều chưa làm tốt trong tổ chức để cùng đưa ra những biện pháp thay đổi kịp thời và tích cực, giúp bảo dưỡng, làm mới và tiếp thêm năng lượng cho Tập đoàn MK vững vàng tiến về phía trước. Nhờ những quyết sách đúng đắn và đúng thời thời điểm, MK Group đã thành công vượt qua những giai đoạn khó khăn đến từ các cuộc khủng hoảng kinh tế, những áp lực trước sự thay đổi nhanh chóng của thị trường, công nghệ, đối tác và chính các đối thủ cạnh tranh để tận dụng tốt cơ hội phát triển và vươn lên thành doanh nghiệp công nghệ cao hàng đầu ASEAN.

Theo ông Nguyễn Trọng Khang, Chủ tịch Hội đồng Quản trị MK Group: “Muốn thành công thì phải thấm nhuần và thực hành tin thần: Không sợ nhìn vào điểm yếu bản thân – Không ngại khi cần thay đổi – Không ngừng đổi mới sáng tạo và Đảm bảo thực hiện những cam kết với Khách hàng – Đối tác”.

Đối phó với Đại dịch Covid-19, MK Group đã có sự chuẩn bị và tập trung nguồn lực để đầu tư vào chiều sâu, mở rộng nhà xưởng, nâng cấp các trang thiết bị máy móc, cải tiến các quy trình sản xuất, tổ chức lại kế hoạch làm việc,... nhằm đảm bảo sự liên tục trong hoạt động sản xuất – kinh doanh. Nhiều hoạt động được thực hiện để đảm bảo việc tuân thủ với các quy định về bảo mật và đảm bảo chất lượng do các tổ chức quốc tế như VISA, MasterCard, JCB, UPI, NAPAS, GSMPL, ISO... đưa ra. Các hệ thống sản xuất, thiết bị kiểm tra chất lượng sản phẩm tân tiến được đầu tư nâng cấp, góp phần tăng công suất thẻ của

Nhà máy MK Smart lên tới hơn 300 triệu thẻ một năm, đặc biệt là công suất thẻ chip giao diện kép (dual-interface). Sản lượng thẻ của MK Smart không chỉ đáp ứng tốt nhu cầu của thị trường trong nước mà còn đẩy mạnh xuất khẩu sang thị trường khu vực và quốc tế. Trong năm 2019, sản phẩm thẻ xuất khẩu sang Nhật Bản của MK Smart đã được Sở công thương Hà Nội bình chọn là 1 trong Top 10 sản phẩm chủ lực của Tp. Hà Nội.



Theo chia sẻ của Chủ tịch HĐQT Nguyễn Trọng Khang, ông và các cộng sự chưa bao giờ nghĩ đến việc dừng bước. “Vào thời kỳ khủng hoảng kinh tế toàn cầu, chúng tôi đã tìm ra những cơ hội của riêng mình. Trong giai đoạn này, trong khi một số công ty không có nguồn lực để mở rộng đầu tư, mua sắm máy móc, phải duy trì hoặc thu nhỏ qui mô thì MK lại nắm bắt cơ hội này để có thể mua sắm thiết bị với chi phí thấp hơn để mở rộng sản xuất. Ngoài ra, chúng tôi đã tăng cường các công tác quản trị, tập trung hơn nữa vào chuyên môn, nhất là những công việc đòi hỏi cao về chất lượng dịch vụ, trình độ và tri thức chuyên sâu để cải tiến nâng cao chất lượng sản phẩm cũng như tăng năng suất lao động”.

Không chỉ vậy, là một tập đoàn công nghệ, hoạt động nghiên cứu và phát triển luôn được ưu tiên tại MK Group. Đây cũng chính là một trong những chìa khóa giúp MK Group đạt được nhiều thành quả đáng ghi nhận trong 21 năm qua. “Trong thế giới phẳng, không nghiên cứu chuyên sâu, không tạo được sự khác biệt thì khó lòng bứt phá.”, ông Khang cho rằng, trở thành người đi trước và làm chủ công nghệ chính là bước đi quan trọng hàng đầu. Hiện nay mỗi năm MK Group dành khoảng 10% doanh thu cho hoạt động R&D. Tất cả hoạt động nghiên cứu và sản xuất của MK đều được thực hiện tại Việt Nam, với hai nhà máy sản xuất thẻ và hai trung tâm R&D ở Hà Nội và Tp. Hồ Chí Minh. Trong khu vực vực ASEAN, MK Group tự hào là công ty hàng đầu về giải pháp xác thực bảo mật số và thẻ thông minh.



“

Trong thế giới phẳng, không nghiên cứu chuyên sâu, không tạo được sự khác biệt thì khó lòng bứt phá.”

MK hiện đang chiếm thị phần lớn thị trường thẻ tại Việt Nam và các sản phẩm Thẻ thông minh của MK hiện diện tại hơn hai mươi quốc gia trên thế giới. Các sản phẩm và giải pháp của MK Group như Giải pháp xác minh và định danh khách hàng MK ABIS, thiết bị FIDO® KeyPass S1, giải pháp xác thực KeyPass OTP, thẻ thông minh đa ứng dụng, ... đã được thị trường đón nhận. Đồng thời, MK Group tiếp tục nghiên cứu, cải tiến và hoàn thiện danh mục các sản phẩm và ứng dụng nhằm đáp ứng tốt nhất những yêu cầu khắt khe của các khách hàng đối tác trong nước và quốc tế, giải quyết nhiều bài toán khó trong vấn đề bảo mật thông tin, thanh toán không tiền mặt, thúc đẩy tiến tới thành phố thông minh, chính phủ điện tử nhằm mang lại một cuộc sống văn minh và an toàn cho người dân.

Chủ tịch HĐQT của MK Group, Nguyễn Trọng Khang cho biết, mục tiêu của MK Group trong chặng đường tới là tiếp tục đẩy mạnh đầu tư cho R&D để đưa ra những sản phẩm, giải pháp mới, đồng thời mở rộng kinh doanh tại châu Á và các châu lục khác như châu Mỹ, châu Phi với định hướng Smart Digital Security – Bảo mật số thông minh. Trong đó, Smart - Phương thức thanh toán, định danh và trao đổi dữ liệu thông minh; Digital - Số hóa các hoạt động định danh và giao dịch; Security - Bảo mật dữ liệu, danh tính và giao dịch.

Có thể nói những thành công của MK Group đến ngày hôm nay chính là dựa trên nền tảng Văn hóa doanh nghiệp vững chắc được Chủ tịch HĐQT Nguyễn Trọng Khang cùng các cộng sự của mình dày công xây dựng. Những giá trị đạo đức “Cam kết – Tin tưởng – Trung thực – Tự trọng và Tôn trọng lẫn nhau” đã trở thành kim chỉ nam cho các hoạt động sản xuất và kinh doanh tại MK Group cũng như góp phần xây dựng nên những mối quan hệ đối tác bền vững của MK Group với các đối tác toàn cầu.

Trong những thời điểm khó khăn của doanh nghiệp khi chịu những tác động tiêu cực từ khủng hoảng kinh tế, dịch bệnh, việc đảm bảo bảo đời sống cho cán bộ nhân viên (CBNV) tập đoàn luôn được đặt lên hàng đầu với những nỗ lực để không cắt giảm nhân sự, đảm bảo thu nhập, mua các gói bảo hiểm bảo vệ thêm cho người lao động, và xây dựng một môi trường làm việc Xanh – Sạch – An toàn cho tất cả CBNV của MK Group. Chiến lược đầu tư vào con người được MK Group thực hiện nghiêm túc thông qua nhiều chương trình đào tạo nâng cao chuyên môn và tay nghề trong nước và quốc tế, hợp tác với các đối tác ở Nhật Bản, Mỹ, Brazil để có những khóa trao đổi, chuyển giao công nghệ nhằm củng cố năng lực cho các Mkers.

Không chỉ làm tốt các hoạt động nội bộ, MK Group còn tham gia và tổ chức nhiều hoạt động thiện nguyện ý nghĩa gồm cả vật chất và trực tiếp tham gia chung tay như giúp các học trò nghèo vùng cao cùng câu lạc bộ Ngân Hạc giấy, Quỹ cơm có thịt, Chương trình Trung thu cho em của Viện Huyết học, Giải chạy Vì trẻ em của ĐSQ Canada, Chạy cho Hội người mù, quyên góp 10 tấn gạo cho Cây gạo NEU của trường ĐH Kinh tế quốc dân nhằm hỗ trợ người khó khăn trong mùa dịch Covid-19... cùng rất nhiều các hoạt động từ thiện thầm lặng khác mà MK đóng góp vì cộng đồng.

Có thể nói sự phát triển và vị thế MK Group đạt được ngày hôm nay chính là thành quả của những nỗ lực không ngừng nghỉ, sự đoàn kết và tin tưởng vào những giá trị Văn hóa doanh nghiệp vững chắc trong suốt những năm qua từ mọi vị trí trong tổ chức. Mong rằng trong những chặng đường tiếp theo của mình, MK Group sẽ vững vàng vượt qua mọi khó khăn, giữ vững vị thế người tiên phong của các doanh nghiệp công nghệ cao Việt Nam và đưa các sản phẩm công nghệ Việt chiếm lĩnh thị phần thế giới.

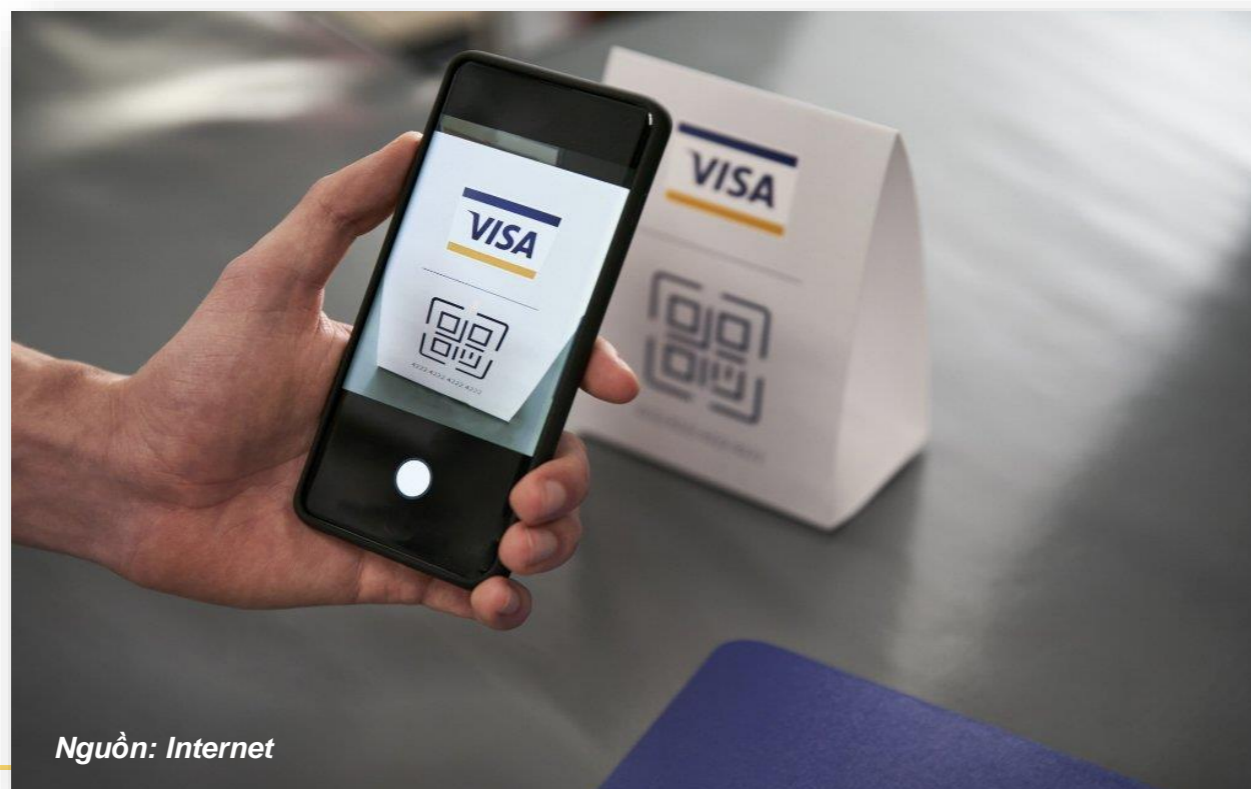
Xin chúc MK Group tuổi 21 “Đổi mới – Sáng tạo - Phát triển bền vững”.

Tỉ lệ sử dụng tiền mặt tại Việt Nam giảm do người tiêu dùng đón nhận những phương thức thanh toán mới

Một khảo sát mới được ủy quyền bởi Visa, công ty công nghệ thanh toán điện tử hàng đầu thế giới, đã ghi nhận người tiêu dùng Việt Nam giảm sử dụng tiền mặt do tăng cường thanh toán kỹ thuật số qua các công nghệ thanh toán mới như thanh toán thẻ không tiếp xúc, thanh toán trên các thiết bị di động và thương mại điện tử.

Khảo sát thái độ thanh toán của người tiêu dùng do Visa thực hiện cho thấy 74% người tiêu dùng tại Việt Nam kỳ vọng sẽ tăng cường thanh toán không tiền mặt trong 12 tháng tới. Đối với nhóm người dùng mang theo ít tiền mặt, lý do chính là vì ngày càng có nhiều nơi chấp nhận thanh toán không tiền mặt.

Những xu hướng này cũng được thể hiện rõ hơn qua các số liệu từ VisaNet, mạng lưới xử lý thanh toán tiên tiến của Visa, với tổng giá trị giao dịch của người tiêu dùng Việt Nam bằng thẻ tín dụng, thẻ ghi nợ Visa tăng 39% và tổng số giao dịch tăng 54%.



Nguồn: Internet

TIN VẤN THẺ NGÂN HÀNG

- Nhân dịp kỉ niệm 63 năm thành lập, từ ngày 23/04/2020 đến 31/12/2020, Ngân hàng Đầu tư & Phát triển Việt Nam (BIDV) triển khai chương trình khuyến mại “Quà tặng khách mới – Giao dịch mọi nơi” với tổng giá trị quà tặng 2.6 tỷ đồng. Theo đó, khi khách hàng đăng ký hoặc mở mới thẻ ghi nợ nội địa, quốc tế và ứng dụng ngân hàng điện tử BIDV SmartBanking đều sẽ nhận được quà tặng có giá trị.
- Từ 1/4/2020 cho đến 30/6/2020, Ngân hàng TMCP Công thương Việt Nam (VietinBank) triển khai Chương trình khuyến mãi (CTKM) “Mở thẻ hoàn tiền - Trúng liền Macbook” với ưu đãi lên đến gần 4 tỷ đồng. Theo đó, khách hàng khi phát hành và chi tiêu thẻ Tín dụng quốc tế (TDQT)/Ghi nợ quốc tế (GNQT) của VietinBank trong thời gian diễn ra CTKM sẽ được hoàn tiền lên đến 1.500.000 đồng và có cơ hội nhận quà tặng hấp dẫn trị giá đến 50 triệu đồng.
- Từ ngày 11/5/2020 cho đến ngày 13/7/2020, Ngân hàng TMCP Công thương Việt Nam (VietinBank) triển khai chương trình khuyến mãi “Gửi tiền, quẹt thẻ - Sống khỏe mỗi ngày” dành cho khách hàng chi tiêu thẻ Tín dụng Quốc tế (TDQT) và thẻ Ghi nợ Quốc tế (GNQT) của Ngân hàng./.

Tỉ lệ sử dụng tiền mặt tại Việt Nam giảm do người tiêu dùng đón nhận những phương thức thanh toán mới (tiếp)

Bà Đặng Tuyết Dung, quản lý khu vực của Visa tại thị trường Việt Nam & Lào cho biết: "Nhiệm vụ của Visa tại Việt Nam là mang đến cho người tiêu dùng những hình thức thanh toán hiệu quả, thuận tiện và an toàn nhất có thể - một mục tiêu phụ thuộc chủ yếu vào việc áp dụng các công nghệ thanh toán mới. Như vậy, thật vui mừng khi kết quả báo cáo đã cho thấy rõ ràng người tiêu dùng Việt Nam đang nhận ra lợi ích mà các công nghệ thanh toán mới có thể mang lại cho họ và áp dụng chúng nhiều hơn với mức giá càng cao hơn."

Một trong những công nghệ mới quan trọng được khảo sát là thanh toán không tiếp xúc – phương thức thanh toán mà người dùng chỉ cần chạm thẻ, điện thoại hoặc các thiết bị đeo vào máy thanh toán POS để thực hiện thanh toán. Hiện tại, có 37% người tiêu dùng đang sử dụng thanh toán thẻ không tiếp xúc tại Việt Nam, và thú vị là có đến 42% người tiêu dùng thực hiện thanh toán không tiếp xúc bằng điện thoại di động.

Đối với nhóm sử dụng thanh toán thẻ không tiếp xúc, có 85% người thanh toán một lần một tuần hoặc nhiều hơn. Khảo sát cũng cho thấy tiềm năng lớn để các công nghệ mới khởi sắc, với bốn trên năm người tiêu dùng chưa từng sử dụng thanh toán thẻ không tiếp xúc có quan tâm đến việc sử dụng phương thức thanh toán này.

84% người dùng cảm thấy thông tin cá nhân của họ được bảo đảm an toàn khi thanh toán qua điện thoại di động. Lướt thanh toán không tiếp xúc trên điện thoại di động, mã QR, và thương mại điện tử đều tăng so với năm 2018 đã chứng minh mức độ tín nhiệm cao từ phía người tiêu dùng. Cụ thể, 82% người dùng sử dụng phương thức thanh toán không tiếp xúc bằng điện thoại di động ít nhất một lần một tuần.

Khảo sát cũng cho thấy các công nghệ thanh toán mới đang thu hút sự quan tâm của người tiêu dùng, với 82% người tiêu dùng Việt Nam cho biết họ quan tâm đến phương thức thanh toán sinh trắc học, chẳng hạn như sử dụng dấu vân tay hoặc xác thực bằng giọng nói để hoàn thành giao dịch, trong khi 81% người dùng quan tâm đến thanh toán thông qua ngân hàng số.

(TuoitreThudo & Vietnam Investment Review)

Datacard® MX9100™ Card Issuance System

Hệ thống cá thể hóa độc đáo vượt trội cho thẻ phẳng nhằm gia tăng sự khác biệt

- Hiện đại hóa quy trình xử lý thẻ thông minh
- Hệ thống mô-đun hoa giúp việc cài đặt diễn ra nhanh chóng và dễ dàng
- Phần mềm quản lý bảo mật cho phép thiết lập và kiểm soát quá trình vận hành thiết bị một cách an toàn và hiệu quả
- Hệ thống quản lý chất lượng nội tuyến tự động giúp loại bỏ các nguy cơ sản phẩm không đạt chất lượng, từ đó giúp tăng năng xuất và giảm chi phí sản xuất
- Công suất phát hành thẻ lên tới 4.000 thẻ/giờ

Hotline: 0903.481.456 - Email: marketing@mkgroup.com.vn






Entrust Datacard ra mắt Certificate Hub với tính năng quản lý vòng đời chứng chỉ của doanh nghiệp

Entrust Datacard (EDC) - nhà cung cấp hàng đầu về công nghệ nhận dạng đáng tin cậy và các giải pháp công nghệ giao dịch bảo mật - vừa ra mắt Certificate Hub, một cổng thông tin cho phép khách hàng tìm kiếm, kiểm soát và tự động hóa các hoạt động triển khai chứng chỉ công cộng và cá nhân thông qua một khung giao diện duy nhất.

Việc sử dụng các chứng chỉ số đã trở nên phức tạp hơn rất nhiều. Những trường hợp sử dụng PKI (Cơ sở hạ tầng khóa công khai) truyền thống như xác thực người dùng và bảo mật VPN hiện cùng song hành với các trường hợp sử dụng như IoT (Internet vạn vật), đóng gói phần mềm và các hệ thống DevOps. Thực tế này đã làm gia tăng số lượng chứng chỉ số nói chung và tạo ra nhu cầu về chứng chỉ ngắn hạn cùng cơ sở hạ tầng phân tán hàng loạt. Do xu hướng tăng mạnh về số lượng chứng chỉ số, các doanh nghiệp phải thực hiện cam kết tự động hóa để tận dụng các phương pháp phát triển ứng dụng và đám mây hiện đại.

“Các doanh nghiệp chú trọng bảo mật có nhu cầu rất lớn đối với giải pháp theo dõi các chứng chỉ và nhận biết thời điểm hết hạn của chúng. Nhiều doanh nghiệp gặp khó khăn trong công tác theo dõi các chứng chỉ và chủ động quản lý chúng, bởi môi trường đã phát triển tới mức quá phức tạp và phân tán để quản lý hàng trăm hoặc hàng nghìn chứng chỉ trên bảng tính, từ đó tạo ra những điểm yếu mà các đối tượng tấn công có thể khai thác”, ông Robyn Westerveldt - Giám đốc Nghiên cứu, Bảo mật & Tín nhiệm tại IDC nhận định. “Một công cụ quản lý vòng đời chứng chỉ như Certificate Hub giúp doanh nghiệp giải quyết sự phức tạp bằng cách tiêu chuẩn hóa, đơn giản hóa và hợp lý hóa công tác phát hiện, quản lý và tự động hóa chứng chỉ”.

Các tổ chức sử dụng Certificate Hub của EDC có được khả năng hiển thị và quản lý các Nhà cung cấp chứng chỉ số (CA) đáng tin cậy cá nhân và công cộng Entrust Datacard, cũng như các Microsoft CA. Nền tảng này sở hữu giao diện dễ sử dụng và trực quan, hoạt động như một điểm thực thi để quản lý tập trung chính sách và các hoạt động quản lý vòng đời chứng chỉ, trong đó có tính năng tìm kiếm hệ thống, cấp chứng chỉ và báo cáo hoàn toàn tự động.

Certificate Hub hoàn toàn tương thích với những sự tích hợp PKI hiện có, do đó, trung tâm này sẽ bổ sung - thay vì phá vỡ - môi trường hiện tại của một tổ chức. Ứng dụng triển khai tại chỗ sử dụng công nghệ điều phối hiện đại cùng các thành phần có thể mở rộng và phát triển trong tương lai nhờ cấu trúc module. Certificate Hub hỗ trợ Trình quản lý bảo mật Entrust (cả mô hình tại chỗ và mô hình do Entrust quản lý), Dịch vụ chứng chỉ Entrust (SSL/TLS) và Microsoft CA.

(Entrust Datacard)

GIẢI PHÁP XÁC THỰC BẰNG MẬT KHẨU MỘT LẦN KEYPASS™ OTP

Giải pháp xác thực bằng mật khẩu một lần KeyPass™ OTP giúp đảm bảo an toàn thông tin cho các hoạt động:

Ngân hàng điện tử | Thương mại điện tử
Giao dịch trực tuyến | Trò chơi trực tuyến



Các thiết bị đi kèm giải pháp gồm:

Thẻ OTP Display (PIN Pad) – OTP Hardware Token (PIN Pad) –
OTP SIM Sticker – OTP Software Token (on Mobile) –
SMS OTP (on Mobile)

MK Group là thành viên của:



HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

Samsung hợp tác với SoFi phát hành thẻ ghi nợ



Nguồn: Internet

Samsung đang hợp tác với ngân hàng số SoFi của Mỹ để ra mắt thẻ ghi nợ Samsung Pay được hỗ trợ bởi tài khoản quản lý tiền mặt.

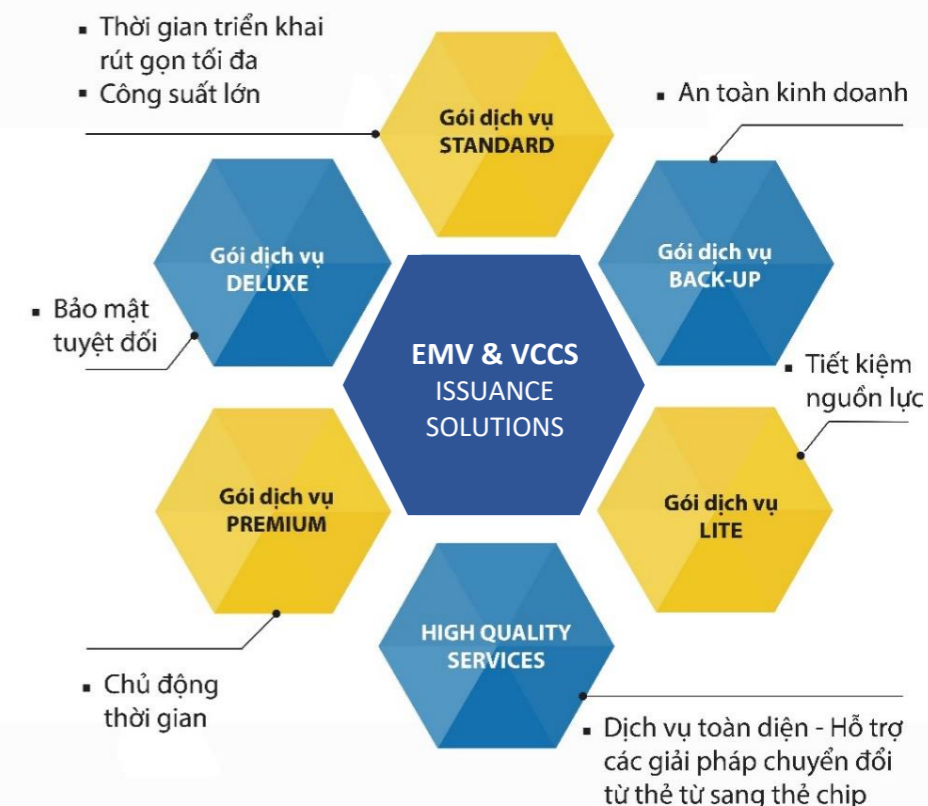
Trong một blog kỷ niệm 5 năm ra mắt dịch vụ thanh toán di động của gã khổng lồ điện tử Hàn Quốc, ông Sang Ahn - Tổng Giám đốc Samsung Pay khu vực Bắc Mỹ cho biết, sản phẩm mới sẽ được giới thiệu vào mùa Hè năm nay.

Blog tiết lộ, Samsung Pay cũng được xây dựng để vượt ra ngoài cách thức mua sắm và thanh toán nhờ “nền tảng quản lý tiền đầu tiên trên thiết bị di động”.

Quyết định lấn sân sang lĩnh vực thẻ thanh toán của Samsung được đưa ra sau khi Apple ra mắt thẻ tín dụng hồi năm ngoái. Ngoài Samsung, Google cũng đang nỗ lực để giới thiệu thẻ ghi nợ mang thương hiệu riêng./.

(Finextra)

MK SMART CUNG CẤP CÁC GÓI DỊCH VỤ PHÁT HÀNH THẺ THEO CHUẨN EMV & VCCS



Garmin tích hợp thẻ giao thông công cộng cho khách hàng Nhật Bản

Garmin mới đây đã thông báo rằng từ nay các chủ sở hữu đồng hồ thông minh Garmin tại Nhật đã có thể tích hợp thêm thẻ giao thông công cộng Suica của họ vào đồng hồ của hãng và sử dụng thẻ này để thanh toán cho các khoản phí di chuyển công cộng và tại các cửa hàng chấp nhận thanh toán Suica.

Dịch vụ này hiện tương thích với các thiết bị Android và iOS và có sẵn cho chủ sở hữu của 10 dòng đồng hồ thông minh Garmin khác nhau.

Theo báo cáo từ Ata Distance, tính đến thời điểm hiện tại thì các phiên bản kỹ thuật số của Suica mới chỉ có sẵn trên iPhone và Apple Watch./.

(NFCWorld)



Nga chuẩn bị áp dụng luật về sử dụng sinh trắc học

Hạ viện Nga (The State Duma) đang lên kế hoạch sẽ đưa luật về sử dụng sinh trắc học áp dụng trong việc cung cấp các dịch vụ tài chính chính thức ra mắt vào tháng 6 sắp tới.



Theo thông cáo, một dự luật về việc sử dụng sinh trắc học trong các dịch vụ tài chính đang được xem xét và có thể sẽ được Hạ viện Nga thông qua vào tháng tới.

Chủ tịch Ủy ban Thị trường Tài chính Anatoly Aksakov nói với Hội đồng Liên bang Nga rằng các lần xem xét dự luật áp dụng sinh trắc học lần thứ 2 và lần thứ 3 sẽ được tổ chức vào tháng 6 sắp tới đây./.

(PlanetBiometrics)

GIẢI PHÁP PHÁT HÀNH THẺ NGAY LẬP TỨC CARDWIZARD



TĂNG TÍNH GẮN KẾT - THÚC ĐẨY DOANH THU

Giải pháp phát hành thẻ ngay lập tức Entrust Datacard® CardWizard giúp thẻ trong trạng thái sẵn sàng sử dụng trong tầm tay của khách hàng chỉ trong vài

Giải pháp sẽ giúp các tổ chức phát hành thẻ:

- Khác biệt hóa thương hiệu
- Tối ưu hóa trải nghiệm của khách hàng
- Tiết kiệm chi phí và giảm thẻ lưu kho
- Bảo mật phát hành ngay lập tức
- Giúp các chương trình Thẻ được triển khai nhanh chóng

HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

Mastercard: Thanh toán không tiếp xúc tăng trưởng mạnh mẽ trên toàn cầu

Nghiên cứu khách hàng của Mastercard cho thấy, khối lượng giao dịch thanh toán không tiếp xúc (TTKTX) trong năm 2020 đã tăng trưởng gấp 2 lần so với khối lượng giao dịch tiếp xúc tại các cửa hàng thực phẩm và dược phẩm.

Trong tháng 2 và 3/2020, do nhiều quốc gia áp đặt các biện pháp hạn chế nhằm tăng cường giãn cách xã hội nên phần lớn người tiêu dùng đã chuyển sang sử dụng TTKTX cho những giao dịch mua hàng thiết yếu. 79% những người được khảo sát trên toàn thế giới cho hay, họ đang sử dụng TTKTX, chủ yếu là do vấn đề an toàn và vệ sinh.

Nghiên cứu thay đổi hành vi tiêu dùng ở 19 quốc gia trên thế giới đã thể hiện bức tranh có gam màu tươi sáng về sự phát triển của TTKTX. Người tiêu dùng trên toàn cầu đã phải tuân thủ các biện pháp giãn cách xã hội và những thách thức mới khác khi mua các mặt hàng phục vụ đời sống thường nhật. Theo Mastercard, sự thay đổi trong hành vi tiêu dùng đặc biệt rõ ràng trong các giao dịch thanh toán, khi mọi người bày tỏ mong muốn thực hiện TTKTX và thể hiện những mối quan ngại về vấn đề vệ sinh và an toàn tại POS.

Một số phát hiện khác bao gồm:

- Nhận thức về vấn đề an toàn và thuận tiện đã thúc đẩy xu hướng ưu tiên sử dụng thẻ TTKTX và nhắc nhở người tiêu dùng về sự tiện lợi của thanh toán một chạm trên toàn cầu. 46% số người được hỏi đã đổi tấm thẻ thanh toán mà họ thường xuyên sử dụng nhất sang thẻ TTKTX.
- Tình trạng gián đoạn trên toàn cầu đã làm gia tăng mối quan ngại từ phía người dùng về việc sử dụng tiền mặt và nhận thức tích cực về TTKTX. 82% số người được hỏi coi TTKTX là phương thức thanh toán đảm bảo vệ sinh hơn, và các giao dịch TTKTX đã tăng trưởng nhanh hơn gấp 10 lần so với những phương thức thanh toán trực tiếp khác.
- 74% số người được hỏi nói rằng, họ vẫn sẽ tiếp tục sử dụng TTKTX trong thời gian sau đại dịch COVID-19/.

(ThePaypers)

SẢN PHẨM THẺ - THẺ THÔNG MINH

MK cung cấp các sản phẩm Thẻ - Thẻ thông minh, giải pháp Phát hành – Cá thể hóa thẻ toàn diện và các ứng dụng thẻ, góp phần tạo nên những chương trình thẻ chất lượng cao và hiệu quả.

- Công nghệ in ấn được chứng nhận bởi các tổ chức quốc tế Visa, MasterCard, JCB, UPI, NAPAS, GSMA, ISO 9001, ISO 14000;
- Sản phẩm phát hành và cá thể hóa trên dây chuyền tiến tiến - hiện đại;
- Cung cấp toàn diện các giải pháp Phát hành – Cá thể hóa - Ứng dụng Thẻ toàn diện và đồng bộ;
- Công suất lớn, đáp ứng nhanh chóng các yêu cầu về tiến độ và thời gian giao hàng;
- Đội ngũ kỹ sư và công nhân chất lượng cao, được đào tạo theo chuẩn quốc tế;



Các chứng chỉ đã đạt:



HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

ABI: 110 triệu thẻ không tiếp xúc sẽ được phát hành vào năm 2020

110 triệu thẻ thanh toán không tiếp xúc sẽ được phát hành bổ sung trong năm 2020 so với kỳ vọng trước khi đại dịch Covid-19, nâng tổng số thẻ được lưu hành toàn cầu lên mức 2 tỷ, theo dự báo từ ABI Research.

"Trên toàn cầu, việc áp dụng thanh toán không tiếp xúc sẽ tăng từ 6% đến 8% so với kỳ vọng trước Covid-19, với mức phát hành được dự báo sẽ tăng 14% so với năm trước, chiếm hơn 65% tổng số thẻ được phát hành trong 2020", các nhà phân tích cho biết.

Thanh toán không tiếp xúc đang là phương thức vệ sinh và càng an toàn hơn để thực hiện thanh toán phạm vi gần và điều này đang được củng cố khi các bên cung cấp trong hệ sinh thái đang chuyển đổi thông điệp tuyên truyền rằng các giao dịch không tiếp xúc sẽ giúp tăng mức độ tiện lợi theo hướng an toàn và đảm bảo sức khỏe.

Giám đốc nghiên cứu Phil Sealy cho biết, cách mà mọi người thanh toán cho mọi thứ đang phát triển và thay đổi nhanh chóng. Và Covid-19 đã thúc đẩy sự thay đổi đáng kể trong thói quen chi tiêu của người tiêu dùng.

Thẻ sinh trắc học :

Khi người tiêu dùng ngày càng sử dụng nhiều hơn và trở nên phụ thuộc hơn vào không tiếp xúc, mối quan tâm về bảo mật và hạn chế gian lận trong việc tăng khối lượng và giá trị giao dịch không tiếp xúc sẽ cần được cân nhắc nhiều hơn.

Thẻ thanh toán sinh trắc học được kỳ vọng sẽ mang lại trải nghiệm thẻ thanh toán không tiếp xúc mà không giới hạn tuyệt nhất cho người tiêu dùng./.



Nguồn: Internet

(Finextra)

MÁY IN THẺ ĐỂ BÀN DATACARD[®]

- Lý tưởng cho các Chương trình Thẻ nhận diện của mọi tổ chức trong các lĩnh vực: Doanh nghiệp, Chính phủ, Trường học, Bệnh viện và các Tổ chức bán lẻ - dịch vụ.
- Các máy in thẻ là sự kết hợp hoàn hảo giữa khả năng in thẻ chất lượng cao và chi phí hợp lý
- Thêm cá tính năng in ấn bảo mật: in mực UV bảo mật, phủ lớp bảo mật, dập dấu nổi giúp các chương trình thẻ trở nên an toàn.
- Phần mềm thân thiện dễ sử dụng
- Vật tư – Phụ tùng chính hãng
- Dịch vụ hỗ trợ kỹ thuật nhanh chóng



Máy in thẻ SD260



Máy in thẻ SD460



Máy in thẻ CD119



Máy in thẻ CR805



Máy in thẻ SD360

HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

HỆ THỐNG PHÁT HÀNH THẺ CÔNG SUẤT LỚN DATACARD® MX

- Lý tưởng cho các tổ chức Phát hành thẻ tầm trung và cao;
- Tính năng toàn diện: Mã hóa thẻ thông minh/dải từ, dập nổi, in chìm, in khắc laser;
- Tùy chọn mô-đun linh hoạt theo yêu cầu đặc thù của từng chương trình thẻ;
- Dịch vụ bảo hành – bảo trì toàn diện

Tình trạng tấn công thiết bị đầu cuối gia tăng mạnh ở châu Âu trong năm 2019

Theo Hiệp hội Giao dịch An toàn châu Âu (EAST), tình trạng tấn công thiết bị đầu cuối đã gia tăng tới 35% trong năm 2019. “Báo cáo Tội phạm Thiết bị đầu cuối châu Âu” được công bố hôm 14/4 cho thấy, hoạt động tấn công gian lận liên quan đến thiết bị đầu cuối đã tăng từ 13.511 vụ lên 18.217 vụ, và phần lớn trong đó là các hành vi tấn công đảo ngược giao dịch ATM với tốc độ gia tăng 87% (từ 4.843 vụ lên 9,054 vụ), trong khi vấn nạn gian lận thẻ giảm 21% xuống mức thấp từ trước đến nay, từ 1.883 vụ xuống còn 1.496 vụ.

EUROPEAN PAYMENT TERMINAL CRIME STATISTICS - SUMMARY						
Terminal Related Fraud Attacks	2015	2016	2017	2018	2019	% +/- 18/19
Total reported Incidents	18,738	23,588	20,971	13,511	18,217	+35%
Total reported losses	€327m	€332m	€353m	€247m	€249m	+1%
ATM Related Physical Attacks	2015	2016	2017	2018	2019	% +/- 18/19
Total reported Incidents	2,657	2,974	3,584	4,549	4,571	+0.5%
Total reported losses	€49m	€49m	€31m	€36m	€22m	-39%
ATM Malware & Logical Attacks	2015	2016	2017	2018	2019	% +/- 18/19
Total reported Incidents	15	58	192	157	140	-11%
Total reported losses	€0.74m	€0.46m	€1.52m	€0.45m	€1.09m	+142%

Source: European Association for Secure Transactions (EAST)

Cũng theo báo cáo của EAST, hoạt động tấn công vật lý liên quan đến ATM chỉ tăng 0,5%, từ 4.549 vụ lên 4.571 vụ. Tình trạng phá và đánh cắp ATM giảm tới 11%, từ 1.256 vụ xuống 1.122 vụ; tấn công ATM bằng chất nổ (gồm khí nổ và chất nổ rắn) giảm 7%, từ 1.052 vụ xuống 977 vụ. Tổng thiệt hại do hoạt động tấn công vật lý liên quan đến ATM gây ra là 22 triệu Euro, giảm 39% so với 36 triệu Euro được báo cáo trong năm 2018.

Thiệt hại tiền mặt bình quân từ một vụ cướp ước tính là 20.369 Euro/vụ, và thiệt hại tiền mặt bình quân từ một vụ tấn công ATM bằng chất nổ là 10.735 Euro/vụ, trong khi thiệt hại tiền mặt bình quân từ một vụ phá hoặc đánh cắp ATM là 9.377 Euro/vụ. Tuy vậy, những con số này không bao gồm hư hại đi kèm đối với thiết bị hoặc tòa nhà, mặc dù đó là những mức thiệt hại lớn và thường vượt quá giá trị của lượng tiền mặt bị mất đi trong những vụ tấn công được thực hiện một cách trót lọt.



Hệ thống công suất tầm trung MX6100, MX2100, MX1100

Hệ thống công suất lớn MX9100, MX8100

HOTLINE
0903.481.456

www.contact@mkgroup.com.vn



EAST đã ghi nhận tổng cộng 140 cuộc tấn công bằng mã độc (malware) và logic nhằm vào ATM trong năm ngoái, giảm 11% so với 157 vụ của năm 2018. Tất cả những cuộc tấn công đều được thực hiện theo hình thức “cash-out” (rút tiền) hoặc “jackpotting” (sử dụng nhiều công cụ để hack vào ATM, khiến máy tuôn ra một lượng lớn tiền mặt). Trong đó, có 118 vụ sử dụng “hộp đen”, và 22 vụ còn lại sử dụng malware. Mặc dù số vụ việc đã giảm xuống, song những thiệt hại liên quan lại cao hơn gấp đôi, từ 450.000 Euro lên 1,09 triệu Euro - tương đương với tỷ lệ gia tăng 142%.

Giám đốc điều hành của EAST, ông Lachlan Gunn nhận xét: “Mặc dù xuất hiện chiều hướng gia tăng tổng thể trong số lượng các vụ gian lận thiết bị đầu cuối, song tổng thiệt hại được báo cáo vẫn không thay đổi. Những thiệt hại do hình thức gian lận đảo ngược giao dịch gây ra thực sự tăng mạnh (từ 2,6 triệu Euro lên 5,2 triệu Euro), song xu hướng giảm xuống của những vụ việc gian lận bằng thiết bị sao chép trái phép thông tin (skimming) đã giúp duy trì mức độ thiệt hại tổng thể ở trạng thái ổn định”.

Báo cáo của EAST cho biết, tổng thiệt hại từ vấn nạn gian lận thiết bị đầu cuối trong năm ngoái là 249 triệu Euro, tăng khoảng 1% so với 247 triệu Euro của 1 năm trước đó. Bên cạnh đó, tổng thiệt hại do hình thức skimming gây ra vẫn không đổi, trong khi thiệt hại từ thủ đoạn bẫy thẻ giảm 14%, từ 2,9 triệu Euro xuống còn 2,5 triệu Euro./.

(ATM Marketplace)

Ukraine công bố dự án hộ chiếu điện tử

Theo thông báo từ Bộ Chuyển đổi Số Ukraine (MDT), chính phủ nước này đã phê chuẩn nghị quyết về dự án thử nghiệm hộ chiếu điện tử (ePassport) trên cổng thông tin dịch vụ công.

MDT lưu ý, ePassport sẽ có giá trị tương tự tài liệu giấy và có thể được sử dụng để di chuyển bằng máy bay hoặc tàu hỏa, tiếp nhận các dịch vụ bưu chính và thực hiện giao dịch ngân hàng trong phạm vi lãnh thổ Ukraine.

Thông báo của MDT cho hay: “Hộ chiếu trên điện thoại thông minh (smartphone) sẽ cho phép người dân không cần phải mang theo thẻ căn cước (ID) và trích lục ID. Nếu bạn không có thẻ ID, chúng tôi đã số hóa hộ chiếu sinh trắc học, và thông tin này cũng xác định danh tính của bạn. Nó mang lại những quyền lợi và khả năng tương tự hộ chiếu giấy có hiệu lực ở trong nước. Số công dân Ukraine có hộ chiếu sinh trắc học hiện cao hơn số lượng công dân có thẻ ID. Điều đó có nghĩa là phần lớn người dân sẽ có thể sử dụng hộ chiếu điện tử để xác thực danh tính”.

Tuy nhiên, MDT nhấn mạnh, tất cả các tài liệu trong ứng dụng di động Action chỉ có hiệu lực ở Ukraine./.

(Security Document World)



Tấn công bề mặt: Mỗi hiểm họa không thể xem nhẹ (Phần 1)

Các đối tượng cần được bảo vệ

Những kẻ xấu thường tìm cách đột nhập vào các tổ chức. Chúng săn tìm những điểm yếu trên các trang web, những máy chủ có dữ liệu bị lộ lọt trên đám mây, và các hệ thống được kết nối trực tiếp với Internet mà chỉ có chút ít hoặc không có bất kỳ sự bảo vệ nào. Các tổ chức cần phải hiểu được khái niệm tấn công bề mặt (tạm dịch từ "surface attack") và ưu tiên những hoạt động có thể giúp thu hẹp bề mặt có thể bị tấn công.



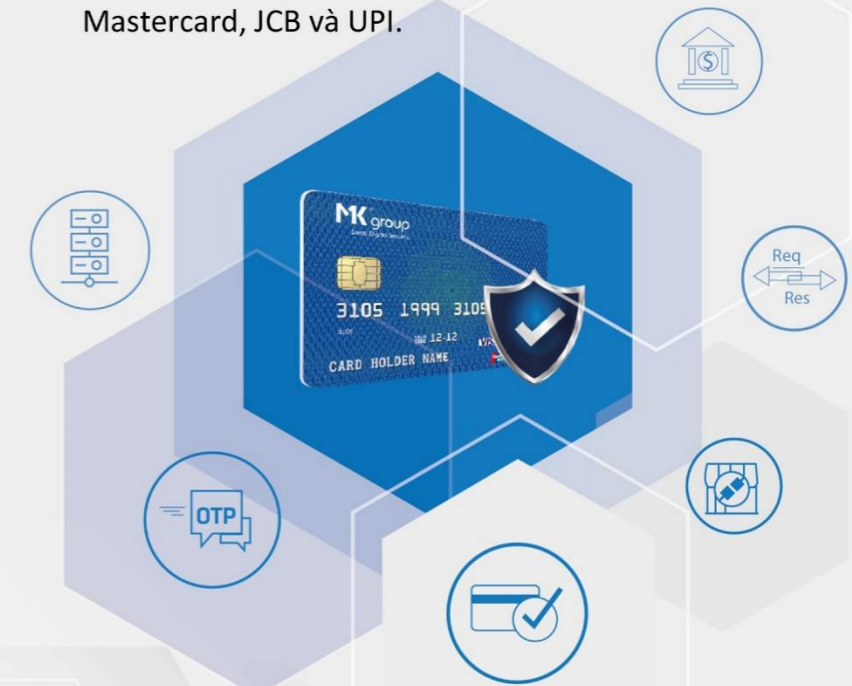
Những bài học thực tế về tác hại của tấn công bề mặt

Hàng chục tổ chức từng chứng kiến những lỗ hổng từ các máy chủ dữ liệu trên đám mây (275 triệu công dân Ấn Độ, 3,4 triệu người Panama, và 600.000 cử tri ở bang Alaska, Mỹ).

WannaCry và NotPetya - 2 loại mã độc tống tiền - đã gây thiệt hại hàng trăm triệu USD thông qua thủ đoạn khai thác các giao thức chia sẻ file SMB công cộng (mà đáng ra không bao giờ được công khai).

GIẢI PHÁP XÁC THỰC GIAO DỊCH THẺ TRỰC TUYẾN EMV 3D SECURE

- Là phương thức bảo mật tiên tiến, giúp bảo vệ chủ thẻ và các đơn vị chấp nhận thẻ tránh các rủi ro trong thanh toán trực tuyến.
- Có thể tích hợp với các phương thức xác thực bằng sinh trắc học, OOB hay OTP.
- Hỗ trợ khả năng xác thực dựa trên mức độ rủi ro (RBA).
- Được chứng nhận bởi EMV Co., Visa, Amex, Mastercard, JCB và UPI.



HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

Ngoài ra còn phải kể đến một cuộc tấn công RDP (Giao thức máy tính từ xa) nhằm vào LabCorp khiến 7.000 hệ thống và 1.900 máy chủ bị lây nhiễm.

Trong tài liệu này, chúng ta sẽ khám phá các nhân tố tạo nên nguy cơ bị tấn công bề mặt, những yếu tố rủi ro lớn và các lỗ hổng nghiêm trọng của một tổ chức, và cách thức để giành lại quyền kiểm soát toàn bộ những điểm yếu nếu bạn bị “đánh đòn”.

Sự hiện diện trên Internet

Các tổ chức có rất nhiều thông tin được đăng tải trực tuyến. Sự hiện diện trên Internet của họ có thể bao gồm các website, thiết bị mạng, ứng dụng di động, dữ liệu LinkedIn, hoặc thậm chí là các đánh giá trên Glassdoor (một cộng đồng nghề nghiệp giúp mọi người tìm kiếm việc làm và các công ty tuyển dụng nhân tài hàng đầu...). Kẻ gian lùng sục trên Internet để tìm kiếm những dữ liệu này hòng hỗ trợ cho những cuộc tấn công. Các lớp dữ liệu được phân chia thành một số hạng mục khác nhau, và một vài hạng mục trong số này có thể không thực sự thuộc về chính tổ chức đó:



Linh hoạt – Đơn giản – Chi phí hợp lý

- Lý tưởng cho các chương trình thẻ ID trong các khối doanh nghiệp, giáo dục, chăm sóc sức khỏe, bán lẻ.
- Sự kết hợp hoàn hảo giữa chi phí, sự bảo mật và tính đơn giản:
 - In thẻ một mặt – sát cạnh
 - In truyền nhiệt trực tiếp
 - In đơn màu, in màu, in trên thẻ ghi xóa
 - Mã hóa dải từ nội tuyến
 - Tốc độ in đủ màu lên tới 150 thẻ/giờ
 - Tốc độ in đơn màu lên tới 500 thẻ/giờ
 - Tốc in cho thẻ in xóa lên tới 14 giây/thẻ
 - Bảo hành 24 tháng



Nguồn: Internet

Hotline: 0903 481 456 Email: marketing@mkgroup.com.vn Website: www.mk.com.vn

Bề mặt có nguy cơ bị tấn công: Bao gồm những bộ phận có thể bị tấn công trực tiếp trong hệ thống của bạn, như các website, thiết bị mạng, và các máy trạm làm việc phục vụ người dùng không được bảo vệ. Nó cũng có thể bao gồm hệ sinh thái không gian mạng rộng lớn hơn của bạn, chẳng hạn như các mạng lưới cung ứng hoặc phụ trợ có thể bị nhắm tới để phục vụ cho một cuộc tấn công.

Bảo vệ thương hiệu: Các ứng dụng độc hại, tên miền được sử dụng để lừa các nhân viên hoặc khách hàng của bạn, và những dịch vụ giả mạo.

Hiểm họa từ thông tin tình báo: Một vài nội dung trong hệ thống dữ liệu rộng rãi của một tổ chức có thể bị phát hiện một cách trực tiếp. Các tin tặc thảo luận về những cuộc tấn công sắp xảy ra trên các diễn đàn web “đen”, mua bán những thông tin định danh cá nhân của các nhân viên trong tổ chức của bạn, hoặc thậm chí là thông tin cá nhân của trợ lý hành chính cho CEO - những đối tượng có thể bị nhắm đến trong các hành động tấn công.

Tất cả 3 nhân tố trên thường đi kèm với nhau, song mỗi nhân tố lại phục vụ một mục đích riêng biệt, và có tầm quan trọng khác nhau. Thí dụ, việc biết được rằng các tin tặc đang nói về âm mưu tấn công tổ chức của bạn trên một diễn đàn ngầm chỉ hữu ích khi bạn có thể thực sự triển khai một số hành động phòng ngừa nguy cơ đó, chẳng hạn như tăng cường đội ngũ nhân viên phụ trách công tác bảo mật nhằm hỗ trợ đối phó với vụ việc, hoặc gửi email cảnh báo tới các nhân viên để nâng cao mức độ cảnh giác đối với những bức thư điện tử được gửi đến.

Tương tự, việc biết được rằng dữ liệu của bạn đã bị lộ lọt có thể hữu ích, song mọi người thường lựa chọn cách ngăn chặn lỗ hổng ở giai đoạn đầu tiên, thay vì trang bị năng lực phát hiện xuất sắc.

Công tác bảo vệ thương hiệu cũng rất khó có thể được thực hiện tốt. Nhiều tổ chức đăng ký hàng nghìn tên miền để phục vụ mục đích phòng ngừa, với những tên miền được chú ý viết sai chính tả và lỗi đánh máy để khiến kẻ gian gặp nhiều khó khăn hơn trong việc khai thác những tên miền này. Nhưng với quá nhiều sự kết hợp tên miền, nỗ lực nắm vững toàn bộ là một nhiệm vụ gần như bất khả thi. Những cuộc tấn công giả mạo thường được tiến hành một cách cực nhanh, với giai đoạn giữa khâu đăng ký tên miền đến gửi thư điện tử chỉ diễn ra trong vòng vài phút, song quy trình phát hiện, cảnh báo và hành động lại có thể lâu hơn rất nhiều. Một chiến lược bảo vệ thương hiệu phổ biến khác là tìm kiếm các hình ảnh logo, nhưng tỷ lệ xác định sai lầm có thể khiến chiến lược này trở thành một nỗ lực phi thực tế.

Các ứng dụng di động giả mạo và những cuộc tấn công thông qua mạng xã hội có thể gây nguy hại, song chúng đòi hỏi nhiều nỗ lực hơn từ những kẻ tấn công và ảnh hưởng lần lượt tới từng nạn nhân (khác với một lỗ hổng dữ liệu trung tâm). Trái lại, bất cứ dịch vụ hệ thống nào không được bảo vệ lại là những quả bom hẹn giờ chỉ trực chờ phát nổ. Đến nay, cuộc tấn công có chi phí rẻ nhất và thành công nhất nhằm vào các tổ chức đơn giản chỉ là sục sạo ở khu vực bên ngoài cho tới khi phát hiện ra một thiết bị không an toàn.

Do số lượng hạn chế về các nguồn tài nguyên sẵn sàng phục vụ mọi nhân viên bảo mật, nên yêu cầu thiết yếu là tập trung vào những nhân tố rủi ro lớn nhất trong quá trình bảo vệ tổ chức của bạn. Dữ liệu cho thấy, đối với nhiều tổ chức, một thiếu sót trong hệ thống bảo mật và phòng ngừa vòng ngoài có thể gây ra số lượng những vụ rò rỉ dữ liệu tồi tệ nhất và ảnh hưởng nghiêm trọng nhất đến kết quả kinh doanh cuối cùng.



Nguyên nhân lớn nhất gây ra những vụ rò rỉ dữ liệu

Với tất cả những công nghệ tiên tiến được phát triển trong thập kỷ qua, người ta dễ sa lãng một số nguyên lý bảo mật cơ bản. Nắm được thông tin về hệ thống của bạn và các thiết bị trên nó là ưu tiên kiểm soát số 1 theo danh sách của SANS/CIS, mặc dù phần lớn các tổ chức không thực hiện bất cứ hoạt động kiểm tra danh sách IP nào trong nhiều năm.

Privacy Rights Clearinghouse là thí dụ điển hình nhất về những vụ rò rỉ dữ liệu. Thống kê đầy sức thuyết phục cho thấy, những vụ đột nhập hệ thống (gồm cả những cuộc tấn công từ bên ngoài và tấn công giả mạo) là hình thức tấn công thường xuyên nhất và gây ra những vụ rò rỉ dữ liệu có thiệt hại lớn nhất. Đáng chú ý, những vụ tấn công vào cơ sở dữ liệu được bảo vệ một cách bí mật nhiều gấp 10 lần so với những vụ tấn công giả mạo. Ngoài ra, số vụ tấn công từ bên ngoài nghiêm trọng hơn gấp 3 đến 4 lần về tần suất và hậu quả so với email giả mạo.

Những đối tượng tấn công thậm chí không cần phải lựa chọn lại hành vi giả mạo hoặc các kỹ thuật tấn công khác bởi có quá nhiều thiết bị được cấu hình sai ở xung quanh chúng. Kẻ gian có thể dễ dàng phát hiện ra những điểm yếu để tính toán cách thức tiếp cận với các tài sản và dữ liệu nhạy cảm. Mở toang cánh cửa để những tài sản này có thể bị tiếp cận từ mạng Internet công cộng cũng tương tự hành động phó mặc cho các máy chủ của bạn ở bên lề đường./.

(Expense)

Mời Quý Độc giả đón đọc phần cuối trong số tiếp theo của **Bản tin Thế Giới Thẻ MK Group**



Copyright© 2020 by MK Group

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