

THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 110 | Tháng 9 - 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

- [Thiết bị Khóa bảo mật FIDO® KeyPass S3 của MK Group đạt chứng nhận FIDO 2 của FIDO Alliance](#)
- [Entrust Datacard bắt tay Deluxe cung cấp giải pháp phát hành thẻ ngay lập tức](#)
- [Thẻ không số nâng cao mức độ bảo mật của thanh toán số](#)
- [Diebold Nixdorf cảnh báo các ngân hàng về phương thức tấn công xâm nhập ATM mới](#)
- [PRIM'X: Giải pháp mã hóa cao cấp bảo vệ thông tin tổ chức, doanh nghiệp](#)



Thiết bị Khóa bảo mật FIDO® KeyPass S3 của MK Group đạt chứng nhận FIDO 2 của FIDO Alliance

Ngày 17/07/2020, sản phẩm Khóa bảo mật (token) FIDO® KeyPass S3 do Công ty Cổ phần Tập đoàn MK (MK Group) sản xuất đã được Liên minh Xác thực FIDO (FIDO Alliance) - trụ sở tại California, Hoa Kỳ cấp chứng nhận cấp chứng chỉ FIDO 2. Sản phẩm token FIDO® KeyPass S3 cho phép người dùng mạng Internet, LAN... có thể an toàn truy cập dịch vụ và thực hiện các thao tác trực tuyến hỗ trợ tính năng FIDO 2.

Với sản phẩm FIDO® KeyPass S3 của MK Group, các tổ chức, doanh nghiệp và người dân có thể chống lại các hành vi gian lận, ăn cắp thông tin truy cập tài khoản trên mạng như skimming (sao chép thông tin tài khoản), phishing (lừa đảo bằng các trang web giả mạo) và man-in-the-middle (tấn công xen giữa).

So với tiêu chuẩn FIDO U2F mà MK Group đã đạt được vào tháng 8 năm 2018 với thiết bị Khóa bảo mật FIDO® KeyPass S1, tiêu chuẩn FIDO 2 có những yêu cầu cao hơn về cấu trúc thiết bị. Ngoài nút bấm vật lý như thiết bị FIDO® KeyPass S1, FIDO® KeyPass S3 còn được trang bị thêm màn hình với vai trò hiển thị các dữ liệu cần xác thực nhằm gia tăng tính an toàn và chính xác trong quá trình thực hiện các hoạt động trực tuyến. Điều này đòi hỏi đội ngũ của MK Group không những phải có chuyên môn, kinh nghiệm vững mà còn cần sự nỗ lực và quyết tâm để tạo ra các sản phẩm công nghệ "Make in Vietnam" đạt chuẩn quốc tế, đáp ứng được những yêu cầu khắt khe đối với các sản phẩm xác thực bảo mật.

Ngoài ra, người dùng khóa bảo mật FIDO® KeyPass S3 còn được hỗ trợ thêm tính năng đăng nhập ứng dụng mà không cần nhập tên tài khoản, mật khẩu và hỗ trợ xác thực đa nhân tố. Theo đó, người dùng nhập mã PIN trước khi khóa bảo mật xác thực thông tin và tạo chữ kí số. Như vậy, cùng với việc không cần cài đặt phần mềm, người sử dụng chỉ cần đơn giản chọn chế độ "thiết lập một khóa bảo mật" có sẵn trong tất cả các trang chủ chấp nhận FIDO 2 (chi tiết các trang hỗ trợ chuẩn FIDO có tại: <https://www.dongleauth.info/>) để đăng kí khóa bảo mật.

Một trong những điểm vượt trội của MK Group trong việc sản xuất và cung cấp các thiết bị khóa bảo mật theo chuẩn FIDO U2F và FIDO 2 chính là việc hỗ trợ các tổ chức doanh nghiệp tích hợp FIDO server (do MK phát triển theo tiêu chuẩn của FIDO) với hệ thống quản lý giao dịch hay truy cập của khách hàng để triển khai các phương



thức xác thực theo chuẩn trong trường hợp website của doanh nghiệp không hỗ trợ xác thực theo chuẩn FIDO Alliance.

Điều này sẽ giúp các tổ chức trong mọi lĩnh vực tài chính, ngân hàng trực tuyến, chính phủ điện tử, thương mại điện tử, lưu trữ dữ liệu đám mây, tài khoản email – mạng xã hội... có thể linh hoạt dễ dàng triển khai sử dụng các thiết bị khóa bảo mật này cho chính nội bộ và khách hàng của mình. Đặc biệt đối với các ngân hàng, các sản phẩm Token FIDO® KeyPass của MK Group còn giúp giải quyết được "bẫy" website giả mạo, chống lại hành vi sao chép bất hợp pháp và tấn công xen giữa trong quá trình giao dịch. Sản phẩm này cũng hoàn toàn đáp ứng được Quyết định 630/QĐ-NHNN về việc "áp dụng các giải pháp về an toàn bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng" cho các giao dịch loại D, giao dịch có giá trị lớn cho cá nhân và doanh nghiệp.

Có thể nói, các thiết bị khóa bảo mật FIDO® KeyPass S1 và FIDO® KeyPass S3 do MK Group sản xuất được kỳ vọng sẽ giúp người dân, các doanh nghiệp cung cấp sản phẩm dịch vụ trên nền tảng Internet, đặc biệt là các tổ chức tài chính ngân hàng sẽ có thêm một công cụ xác thực dành cho khách hàng của mình; đảm bảo yếu tố an toàn - bảo mật, tiện dụng - đơn giản, giá thành hợp lý và dễ triển khai./.

Thanh toán không tiếp xúc đang ngày càng trở nên phổ biến



Nguồn: Internet

Dữ liệu từ Khảo sát về Thái độ Thanh toán của Người tiêu dùng Việt Nam do Visa thực hiện gần đây (dựa trên cơ sở so sánh dữ liệu từ tháng 1 đến tháng 6/2020 với dữ liệu trong giai đoạn cùng kỳ năm 2019 của VisaNet) cho thấy, 37% người tiêu dùng Việt Nam hiện thanh toán bằng thẻ không tiếp xúc. 85% những người trong tập khách hàng này cho biết họ thường sử dụng phương thức thanh toán không tiếp xúc (TTKTX) ít nhất 1 lần/tuần.

Cũng theo Visa, với phương thức trên, người tiêu dùng có thể chạm để trả tiền tại bất cứ quầy thanh toán nào có biểu tượng TTKTX mà không cần đưa thẻ cho nhân viên thu ngân. TTKTX được bảo mật mạnh mẽ bởi công nghệ chip EMV. Thẻ TTKTX được tích hợp một đầu ăng ten nhỏ có thể đọc được bởi một máy POS trong khoảng cách tối đa 4 cm. Trong toàn bộ quá trình thay toán, tấm thẻ không bao giờ rời khỏi tay chủ sở hữu, và giao dịch diễn ra cực kỳ nhanh chóng bởi POS chỉ mất chưa đến nửa giây để đọc thẻ hoặc thiết bị không tiếp xúc. Người tiêu dùng còn có thể sử dụng điện thoại di động, nhập PIN, mật khẩu hoặc thông tin sinh trắc học để tăng thêm mức độ bảo mật.

Phương thức thanh toán mới mẻ này mang lại lợi ích cho cả người tiêu dùng và đơn vị chấp nhận thẻ. Nhờ tốc độ nhanh chóng của TTKTX, người tiêu dùng giảm đến mức tối thiểu thời gian chờ đợi và kiểm soát giao dịch một cách tốt hơn vì tấm thẻ luôn nằm trong tay của chính họ. Các đơn vị chấp nhận thẻ cũng giành được lợi thế khi có thể phục vụ được nhiều khách hàng hơn, cắt giảm chi phí xử lý tiền mặt, từ đó mang lại trải nghiệm thanh toán tích cực hơn cho khách hàng. TTKTX đặc biệt hữu dụng trong bối cảnh đại dịch COVID-19 đang lan rộng trên toàn cầu và bùng phát trở lại ở Việt Nam.

Theo thống kê, các giao dịch TTKTX của Visa trong 6 tháng đầu năm 2020 đã tăng trưởng hơn 500% so với cùng kỳ năm 2019. Tổng giá trị giao dịch không tiếp xúc của Visa cũng tăng trưởng hơn 600% trong cùng kỳ. Dự báo, những con số kỷ lục này sẽ tiếp tục được giữ vững và tái lập thêm nhiều kỷ lục trong giai đoạn tới, bởi ngày càng nhiều tổ chức được trang bị đầu đọc thẻ TTKTX nhằm cung cấp phương thức thanh toán an toàn trong đại dịch, cũng như để theo kịp công nghệ tối tân này trên thế giới./.

(Intellasia)

TIN VẤN THẺ NGÂN HÀNG

- Từ ngày 14/08 cho đến hết tháng 12 năm 2020, Ngân hàng TMCP Sài Gòn Thương Tín (Sacombank) triển khai chương trình ưu đãi hoàn tiền và cơ hội trúng thưởng iPad Pro 11 Inch 128 GB Wifi cho khách hàng mở mới và sở hữu thẻ Sacombank Mastercard.
- Từ ngày 17/08 cho đến hết 17/09/2020, Ngân hàng TMCP Sài Gòn Thương Tín (Sacombank) và Tiki triển khai chương trình khuyến mãi dành cho chủ thẻ tín dụng Sacombank Tiki Platinum. Cụ thể, Sacombank Tiki Platinum khi chi tiêu tại Tiki (website: www.tiki.vn hoặc ứng dụng Tiki) và các đơn vị chấp nhận thẻ khác đạt từ 30 triệu đồng (được cộng dồn), chủ thẻ sẽ nhận một mã tham dự quay số để có cơ hội trúng một trong 10 coupon điện tử trị giá 29,99 triệu đồng.
- Ngân Hàng Thương Mại Cổ Phần Kỹ Thương Việt Nam từ ngày 16/07/2020 cho đến hết ngày 30/09/2020 triển khai chương trình ưu đãi du lịch dành cho các chủ thẻ Techcombank Visa. Cụ thể, các chủ thẻ khi thanh toán du lịch tại Agoda/ Traveloka/ Trip.com/ Ivivu/ Klook/ KKDay/ Vinpearltravel.vn. đều sẽ được nhận ưu đãi hoàn tiền 15% ./.

(Tổng hợp từ Internet)

75% người tiêu dùng Mỹ thích dùng thẻ thanh toán không tiếp xúc

Cuộc khảo sát do Entrust Datacard thực hiện đối với 1.000 người tiêu dùng Mỹ quen thuộc với thẻ thanh toán không tiếp xúc (TTKTX) cho thấy, 75% trong số này thích sử dụng thẻ TTKTX làm phương thức thanh toán chính. Vệ sinh (70%) và tốc độ xử lý (67%) là những lý do hàng đầu dẫn đến sự ưa chuộng của những người tham gia khảo sát.

Tỷ lệ sử dụng nhiều nhất rơi vào nhóm người tiêu dùng thuộc các thế hệ Gen Z, Millennial và Gen X, khi đặt cạnh thế hệ Baby Boomer. Cụ thể, 20% người tiêu dùng thuộc thế hệ Baby Boomer chưa bao giờ sử dụng tính năng TTKTX trên thẻ ghi nợ hoặc thẻ tín dụng khi mua hàng, trong khi tỷ lệ này chỉ ở mức dưới 10% trong 3 thế hệ còn lại.

Nhìn chung, 83% số người được khảo sát tin rằng họ vẫn sử dụng thẻ TTKTX, và 61% cho rằng tính năng TTKTX ít nhất là một ưu thế dành cho thẻ tín dụng hoặc thẻ ghi nợ của họ./.

(NFCW)



Datacard® MX9100™ Card Issuance System

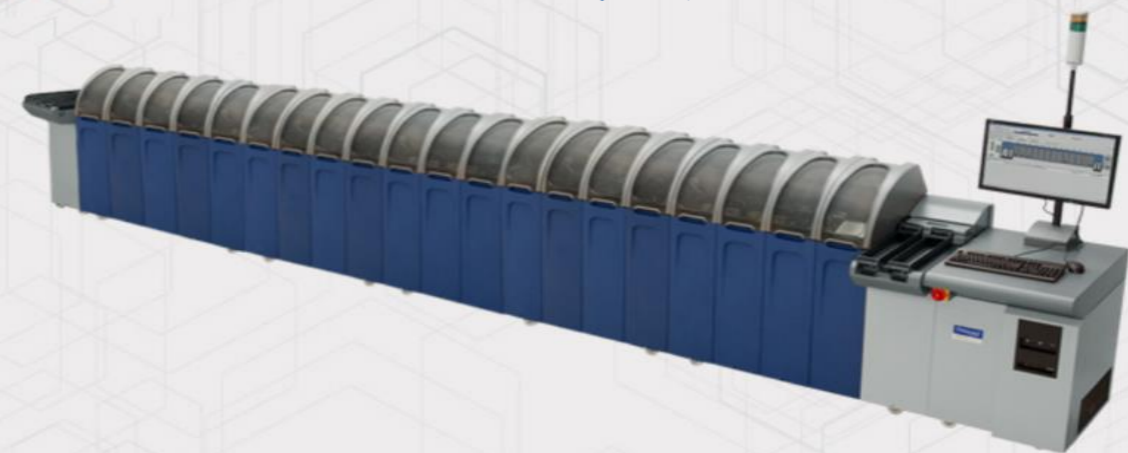
Hệ thống cá thể hóa độc đáo vượt trội cho thẻ phẳng nhằm gia tăng sự khác biệt

- 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

MKgroup
Smart Digital Security

Entrust Datacard™



Entrust Datacard bắt tay Deluxe cung cấp giải pháp phát hành thẻ ngay lập tức



Nguồn: Internet

Entrust Datacard vừa ký thỏa thuận với Deluxe, công ty cung cấp giải pháp đáng tin cậy cho doanh nghiệp (Trusted Business Solutions™), để mang đến cho các khách hàng của Deluxe quyền truy cập vào danh mục toàn diện, trong đó có giải pháp phát hành thẻ tài chính ngay lập tức. Theo thỏa thuận, Deluxe sẽ tiếp thị giải pháp phát hành ngay lập tức của Entrust Datacard để giúp các khách hàng tài chính của công ty củng cố các mối quan hệ khách hàng.

Các tổ chức tài chính đang nỗ lực thay đổi trải nghiệm khách hàng sau đại dịch COVID-19, đáp ứng nhu cầu về thời gian quay vòng nhanh hơn, dịch vụ không chạm nhiều hơn, cùng những loại thẻ tín dụng và thẻ ghi nợ không tiếp xúc mới. Với giải pháp phát hành ngay lập tức thẻ tín dụng và thẻ ghi nợ, khách hàng có thể nhận ngay tấm thẻ đã được kích hoạt với đầy đủ thông tin cá nhân khi mở tài khoản, hoặc khi thay thế thẻ bị mất hay bị đánh cắp.

Dịch vụ này mang đến trải nghiệm tùy chỉnh theo yêu cầu mà khách hàng đang tìm kiếm từ các tổ chức tài chính. Giải pháp phát hành thẻ ngay lập tức của Entrust Datacard cung cấp tính linh hoạt cần thiết cho các ngân hàng và hiệp hội tín dụng để tạo ra trải nghiệm tích cực và chuyển đổi thành viên thành những người ủng hộ.

Deluxe đã nhận thấy cơ hội to lớn để giúp các tổ chức tài chính phát triển với giải pháp phát hành ngay lập tức, được hỗ trợ bởi những dịch vụ hàng đầu và hướng dẫn chuyên sâu từ Entrust Datacard, cho phép các ngân hàng nâng cao trải nghiệm khách hàng. Giờ đây, các tổ chức tài chính có thể mang đến cho khách hàng sự an tâm trong thời gian dài./.

(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:

Mercedes tích hợp tính năng thanh toán sinh trắc học trên xe sang S-Class



Nguồn: Internet

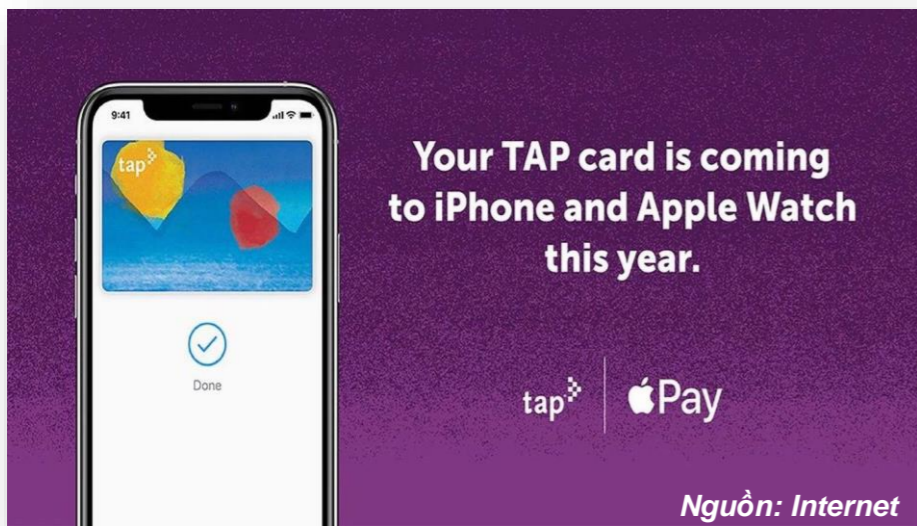
Hệ thống thông tin giải trí trên dòng sedan S-Class mới của Mercedes sẽ được tích hợp các tính năng sinh trắc học như nhận dạng vân tay, giọng nói, và tùy chọn nhận dạng khuôn mặt, cho phép “xác thực các quy trình thanh toán số từ xe”.

Theo thông báo của hãng xe Đức, bảng điều khiển của S-Class thế hệ mới sẽ được tích hợp cảm biến vân tay và “có thể tùy chọn 2 camera” để nhận dạng khuôn mặt./.

(NFCW)

LA Metro sắp cho phép hành khách bổ sung thẻ giao thông TAP vào Apple Pay

LA Metro thông báo, hành khách sử dụng phương tiện công cộng ở Los Angeles có thể bổ sung thẻ giao thông TAP vào iPhone hoặc Apple Watch “trong năm nay”.



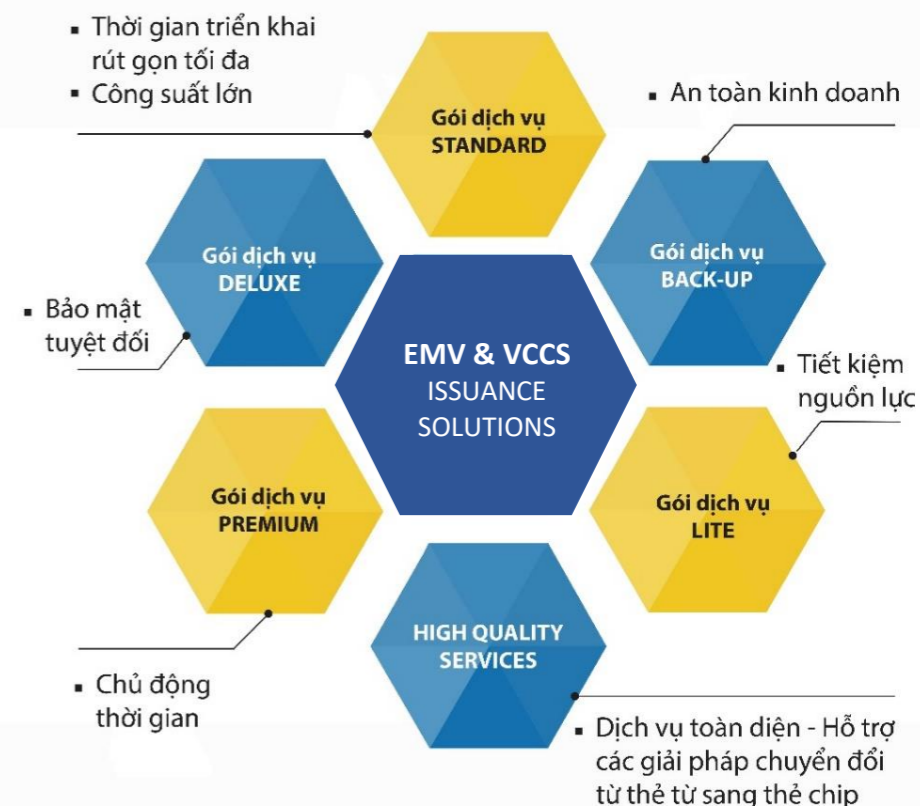
Nguồn: Internet

Sau khi triển khai, LA Metro sẽ cùng với các thành phố New York, Portland và Chicago cung cấp dịch vụ trên tại Mỹ.

Trên bình diện quốc tế, dịch vụ này được hỗ trợ ở Trung Quốc đại lục, Hong Kong, London, Singapore, Vancouver, Sydney, và các thành phố của Nga như Moscow, St Petersburg và Novosibirsk, và trên thẻ Suica ở Nhật Bản./.

(NFCW)

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



Thẻ không số nâng cao mức độ bảo mật của thanh toán số

Thẻ không số, là loại thẻ không hề có bất kỳ số hay mã nào hiển thị trên bề mặt, đang cách mạng hóa thanh toán số bằng cách khiến cho những giao dịch này trở nên an toàn hơn.

Khi chúng ta hướng tới một nền kinh tế không dùng tiền mặt, việc đầu tư vào hệ thống tích hợp công nghệ bảo mật ngày càng trở nên quan trọng hơn. Một bước đi trong xu hướng đó là thẻ không số. Những mẫu thẻ này sẽ không có bất kỳ con số hay mã nào được in trên bề mặt, nhờ đó giúp nâng cao khả năng bảo mật cho người dùng. Nếu khách hàng vô tình làm mất thẻ, nguy cơ bị lộ thông tin cá nhân nếu rơi vào kẻ xấu sẽ giảm đi.

Để xác thực thanh toán, khách hàng chỉ cần nhập mã PIN, thường chỉ sử dụng một lần, vì vậy hạn chế được khả năng gian lận. Một số thẻ không số cũng cho phép sử dụng các hình thức xác thực khác ngoài mã PIN. Bên cạnh đó, hầu hết thẻ không số đều được kết nối với ứng dụng của chúng trên điện thoại của người dùng, giúp đơn giản hóa quy trình hủy kích hoạt.

Gần đây, thị trường Ấn Độ đã chứng kiến đợt phát hành thẻ không số đầu tiên. FamPay - ngân hàng di động dành cho thanh thiếu niên, chuyên cung cấp các lựa chọn giao dịch không dùng tiền mặt - đã tung ra FamCard. Loại thẻ này tương tự thẻ tín dụng, song chủ thẻ có thể sử dụng để thực hiện thanh toán một cách độc lập, giúp các phụ huynh bớt gặp khó khi phải đưa tiền mặt hoặc thẻ ghi nợ và tín dụng cho con cái.



Nguồn: Internet

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



Nguồn: Internet

Với FamCard, trẻ vị thành niên có thể thanh toán trực tuyến, cũng như ngoại tuyến, mà không cần phải lập tài khoản ngân hàng. Mọi giao dịch được thực hiện thông qua FamCard đều được bảo vệ. Các thông tin thiết yếu sẽ được lưu trữ trong ứng dụng FamCard trên điện thoại của người dùng. Loại thẻ không số này, nếu bị thất lạc hoặc bị đánh cắp, có thể dễ dàng bị vô hiệu hóa bằng ứng dụng.

Gã khổng lồ công nghệ Apple cũng đã phát hành thẻ tín dụng không số, một phần của các dịch vụ Apple Pay. Thẻ hỗ trợ người dùng thực hiện các giao dịch mua hàng thông qua iPhone hoặc đồng hồ thông minh Apple Watch. Sản phẩm này sử dụng Touch ID để hạn chế nguy cơ gian lận. Mặc dù không có số hiển thị trên thẻ, nhưng nó được lưu trữ trong ví kỹ thuật số được liên kết với thẻ trên điện thoại của người dùng.

Tiếp bước Apple, Curve - doanh nghiệp thẻ tín dụng và ứng dụng - hồi tháng 4/2020 cũng đã ra mắt thẻ không số. Số của thẻ được lưu trữ bên trong phần mềm và khách hàng có thể truy cập thông qua ứng dụng Curve. Thẻ có thể hoạt động tại mọi quốc gia chấp nhận MasterCard và có quy trình xử lý thanh toán không tiếp xúc, chip, PIN và dải từ.

Banco Santander - ngân hàng thương mại đa quốc gia của Tây Ban Nha - cũng tham gia cuộc chơi bằng cách phát hành thẻ tín dụng không số đầu tiên ở Mexico. Sản phẩm chỉ hiển thị tên chủ thẻ và ngày hết hạn. Banco Santander cho biết, loại thẻ này giúp giảm tới 90% nguy cơ gian lận.

Cũng tại Tây Ban Nha, ngân hàng Orange Bank cũng đã phát hành thẻ ghi nợ số hóa nhằm giúp khách hàng có thể thực hiện những giao dịch thanh toán di động ngay lập tức bằng cả hình thức trực tuyến và tại cửa hàng. Khách hàng cũng có thể yêu cầu phát hành kèm một chiếc thẻ "truyền thống" được nâng cấp bảo mật nhờ việc trên thẻ không hề có bất kỳ thông tin số thẻ, mã CVC hay ngày hết hạn.

Thẻ không số đang từng bước cách mạng hóa thanh toán số và khiến cho những giao dịch này trở nên an toàn hơn. Trên thực tế, việc một người có thể dễ dàng chặn thẻ bằng ứng dụng an toàn trên điện thoại sẽ làm cho nó hiệu quả gấp đôi./.

(Financial Express)

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

Diebold Nixdorf cảnh báo các ngân hàng về phương thức tấn công xâm nhập ATM mới

Diebold Nixdorf đang cảnh báo các cửa hàng, ngân hàng và khách hàng về hình thức tấn công mới dựa trên phần cứng “jackpotting”, thuật ngữ trong ngành chỉ những cuộc tấn công mà kẻ gian sử dụng để nhanh chóng vét sạch tiền trong ATM.

Biến thể mới sử dụng một thiết bị điều hành phần mềm stack độc quyền của Diebold Nixdorf. Những kẻ tấn công sau đó kết nối thiết bị với ATM và ra lệnh.

Những cuộc tấn công trót lọt khiến ATM tự động nhả tiền, đôi khi có tốc độ lên đến 40 tờ tiền mặt trong 23 giây. Các thiết bị được gắn bằng cách truy cập vào chìa khóa mở ATM hoặc khoan lỗ hay phá khóa để tiếp cận bên trong thân máy.

Trong những cuộc tấn công jackpotting trước đây, các thiết bị được gắn - gọi là “hộp đen” - thường kích hoạt các giao diện lập trình trong hệ điều hành ATM để chuyển lệnh đến phần cứng nhả tiền.

Theo Diebold Nixdorf, ngày càng có nhiều cuộc tấn công nhắm vào các thiết bị đầu cuối ProCash của công ty, đặc biệt là mẫu ProCash 2050xs USB. Đáng chú ý, những cuộc tấn công đang tiếp tục diễn ra ở “một số quốc gia châu Âu”./.

(Payments Cards & Mobile)



Nguồn: Internet

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

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

Visa triển khai tính năng thanh toán không tiếp xúc trên hệ thống giao thông công cộng tại 500 thành phố



Visa đã triển khai tính năng thanh toán không tiếp xúc (TTKTX) trên các phương tiện giao thông công cộng tại hơn 500 thành phố để hỗ trợ nhu cầu ngày càng lớn về những cách thức đi lại an toàn hơn.

Theo Business Insider, Visa đang phối hợp với Cubic Transportation Systems phát hành thẻ TTKTX tại London, Miami, New York, Sydney, và Vancouver. Bên cạnh đó, dự án chạm-để-thanh toán của Visa đã có mặt tại Brussels, Bratislava, Bucharest, Hong Kong, Santo Domingo, và Turin.

Sáng kiến trên giúp đáp ứng nhu cầu ngày càng lớn về những phương thức thanh toán an toàn hơn và TTKTX, bởi vì đã có thông tin cho rằng 65% tổng số thẻ trên thị trường sẽ có tính năng không tiếp xúc vào cuối năm 2020.

Hơn nữa, sự bùng phát của đại dịch COVID-19 đã nâng cao nhận thức về TTKTX ở hầu hết các thị trường thuộc châu Âu, trong khi mức độ phổ biến ở Mỹ là tương đối thấp - tương tự trường hợp của thẻ chip khi lần đầu tiên được ra mắt.

Tuy nhiên, khi người tiêu dùng phải vật lộn với những nỗi lo về sức khỏe cá nhân, TTKTX có thể trở thành một phương thức thanh toán được ưa chuộng, vì nó an toàn và tiện lợi hơn. Thí dụ, nếu khách hàng không có thẻ TTKTX, họ vẫn có thể nạp thẻ vào ví di động và đặt bảo mật vân tay để sử dụng ngay./.

(ThePaypers)

PRIM'X: GIẢI PHÁP MÃ HÓA CAO CẤP BẢO VỆ THÔNG TIN TỔ CHỨC, DOANH NGHIỆP

Ngày nay, các tổ chức và doanh nghiệp đang sở hữu một khối lượng thông tin rất lớn, quan trọng và nhạy cảm. Đó có thể là một chiến lược kinh doanh của tập đoàn, một bản nghiên cứu thiết kế sản phẩm đang phôi thai, cũng có thể là các dữ liệu công dân liên quan đến thông tin thẻ căn cước, hộ tịch, đất đai, bảo hiểm, hồ sơ bệnh án cá nhân, tài chính hoặc thống kê tài sản của các chính khách... Những thông tin này đang được khởi tạo, lưu trữ, lưu chuyển qua hệ thống nội bộ, cũng như không gian mạng, một cách liên tục và hầu hết đang tồn tại dưới dạng không mã hóa (Clear text). Những thông tin này chính là tài sản số vô cùng quan trọng, nếu bị thất thoát, đánh cắp, phát tán, sẽ gây ra thiệt hại nặng nề, ảnh hưởng không nhỏ đến hoạt động kinh doanh và uy tín của doanh nghiệp.

Các doanh nghiệp hiện tập trung nhiều vào công tác chống tấn công từ bên ngoài vào hệ thống bằng cách xây dựng hệ thống tường lửa, chống virus, các giải pháp phân tích đối phó tấn công (SOC, SIEM), chống thất thoát dữ liệu như DLP, DRM... Tuy nhiên, theo các thống kê quốc tế, rủi ro có thể đến ngay từ hệ thống công nghệ thông tin (CNTT) truyền thống. Các dữ liệu khởi tạo từ máy của người dùng đều đang lưu lại trên lịch sử ổ "C" (local file, user profile, temporary file, browser cache...), được lưu trữ và chia sẻ trên các định dạng ổ cứng NAS, Server, trên Cloud (OneDrive, Dropbox...). Các thông tin cũng được lưu chuyển qua email, được sao chép sang các thiết bị di động như USB, ổ cứng rời... Theo cấu trúc truyền thống, bộ phận CNTT đang quản trị không chỉ các phần mềm mà truy cập được cả thông tin cá nhân và doanh nghiệp do dữ liệu tồn tại dưới dạng không mã hóa, và đây cũng chính là một rủi ro lớn. Nhìn chung, các dữ liệu của chúng ta đang tồn tại ở khắp nơi và có thể trở thành mục tiêu tấn công của đối thủ vào bất cứ lúc nào, từ nhiều điểm khác nhau.

PRIMX

MAKE ENCRYPTION HAPPEN

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

MK Group, với hơn 21 năm kinh nghiệm về giải pháp bảo mật và thẻ thông minh, đang cung cấp giải pháp mã hóa dữ liệu toàn diện của Prim'X - một giải pháp mang tính tổng thể, an toàn, dễ sử dụng. Giải pháp có khả năng vận hành một cách tự động và dễ dàng tích hợp với các hạ tầng, chính sách bảo mật sẵn có của các tổ chức và doanh nghiệp: đảm bảo mã hóa mọi nơi, mọi lúc.

Những giải pháp mã hóa dữ liệu toàn diện của Prim'X tập trung mã hóa các dữ liệu lưu trữ (Data at rest) hoặc dữ liệu di chuyển (data in transit) thông qua tính năng quản lý quyền được hiểu thông tin (Rights to Understand). Nhân viên CNTT là người quản trị phần cứng, cài đặt phần mềm, phân quyền, nhưng sẽ không đọc hiểu được thông tin trên hệ thống. Trong khi đó, nhân viên phụ trách bảo mật (Security officer) mới là người soạn thảo, triển khai, áp đặt các chính sách an toàn thông tin (GPO) của doanh nghiệp. Giải pháp mã hóa của Prim'X có thể hoạt động được trên từng máy cá nhân, hoặc đồng bộ trên quy mô lớn thông qua ActiveDirectory một khi các máy cá nhân được kết nối nội bộ với DC. Đối với góc nhìn phía người dùng, mọi thao tác làm việc trên các phần mềm văn phòng vẫn không thay đổi (Seamless), hoạt động mã hóa diễn ra ngầm từ phía người dùng (Client side), một cách tự động (Automatically) và ngay tức thì (On the fly). Phần mềm Prim'X chiếm ít tài nguyên và hầu như không ảnh hưởng đến tốc độ hoạt động của máy. Người dùng được cấp khóa để bảo vệ dữ liệu cá nhân và có trách nhiệm quản lý khóa cá nhân của mình.

Prim'X sử dụng những thuật toán mã hóa tiên tiến nhất như AES 256 bits, RSA 2048 bits, tương thích với các PKI chính (X509), Token hoặc thẻ thông minh (Smart card), tích hợp dễ dàng với các hạ tầng sẵn có như ActiveDirectory, SCCM...

Prim'X khẳng định khả năng bảo vệ mạnh mẽ và tin cậy thông qua hệ thống chứng chỉ EAL3+ Common Criteria, Cơ quan An toàn thông tin Pháp (ANSSI) & Security Visa, NATO Restricted, EU Restricted, và đặc biệt là đã được Ban Cơ yếu Chính phủ Việt Nam cấp phép kinh doanh cho sản phẩm Mật mã dân sự. Sản phẩm của Prim'X đang nhận được sự quan tâm lớn từ các tổ chức, doanh nghiệp Việt Nam có nhu cầu bảo vệ thông tin nội bộ trước những cuộc tấn công thông tin ngày nay.

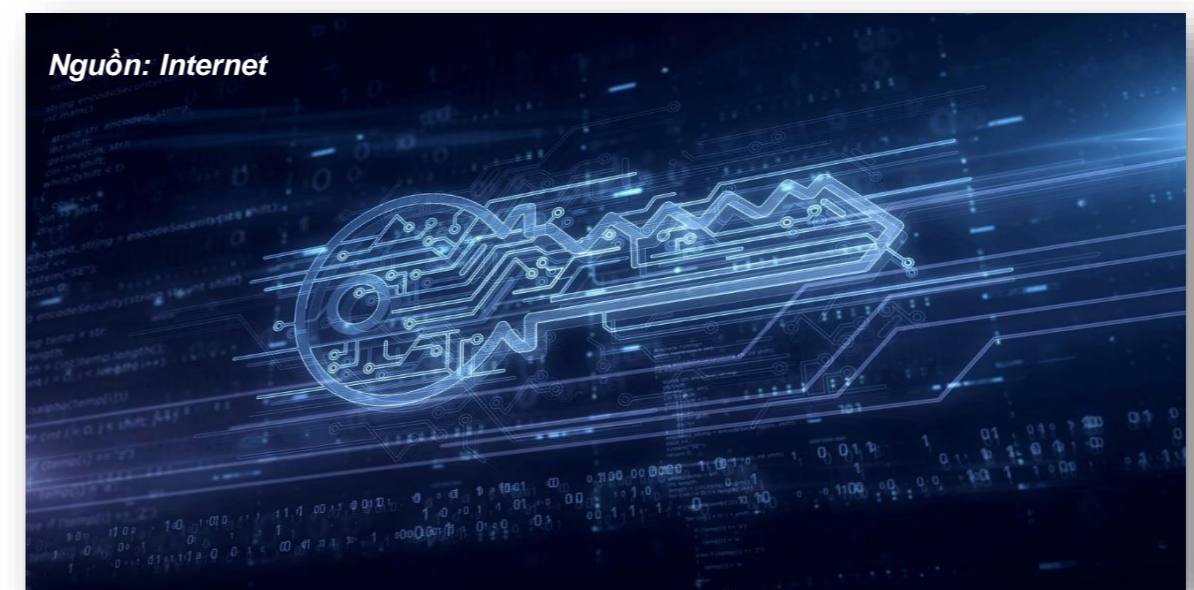
Các sản phẩm chính của Prim'X:

- ZoneCentral:** phần mềm này được cài đặt trên các máy người dùng để mã hóa thông tin trên máy trạm (local file, user profile, temporary files, browser cache..), mã hóa thông tin khi người dùng lưu và chia sẻ trên máy chủ, ổ SAN, NAS...Người dùng làm việc hoàn toàn trên môi trường mã hóa, không lưu khóa trên hệ thống. Chính sách an toàn thông tin nội bộ do Nhân viên phụ trách ATTT (CISO) soạn thảo, triển khai, áp dụng. CISO cũng quản lý quyền đọc hiểu giữa những người dùng, các nhóm và bộ phận. ZoneCentral mang lại mức độ bảo mật cao bằng cách mã hóa dữ liệu và chỉ cấp quyền đọc hiểu cho người có thẩm quyền và liên quan; sử dụng thuật toán AES (128 đến 256 bits) và RSA (1024 đến 4096 bits), và chạy trên hệ điều hành Windows 7 đến 10; hỗ trợ các ngôn ngữ Anh, Pháp, Đức, Tây Ban Nha.
- ZED:** phần mềm được sử dụng để mã hóa nội dung khi sao chép lên các thiết bị lưu trữ rời để trao đổi với nhau hoặc để đính kèm email. Cách sử dụng ZED tương tự sử dụng file "*.zip" của Windows. Người dùng chỉ cần nhấp chuột để tạo Folder và Add các file, quá trình mã hóa sẽ diễn ra tự động. ZED có thể nén file để giảm dung lượng. Phần mềm này sử dụng mật khẩu hoặc chứng thư RSA. Trong trường hợp mất khóa, CISO có thể khôi phục các file đã mã hóa. Người dùng bên ngoài tổ chức không cài đặt ZED

hợp mất khóa, CISO có thể khôi phục các file đã mã hóa. Người dùng bên ngoài tổ chức không cài đặt ZED có thể sử dụng phần mềm miễn phí “Zed!Free” để nhận, đọc sửa, và gửi lại. ZED sử dụng thuật toán AES (128 đến 256 bits) và RSA (1024 đến 4096 bits), chạy trên hệ điều hành Windows 7 đến 10, Linux và Mac OS, và có sẵn 7 ngôn ngữ. Ứng dụng miễn phí “Zed!Mobile” có thể chạy trên iOS và Android.

3. **ZEDMAIL:** Phần mềm mã hóa thư điện tử dành cho doanh nghiệp. Người dùng sử dụng email một cách bình thường, trong khi nội dung và file đính kèm được mã hóa tự động. Ở phía người nhận, email được giải mã tái tạo nguyên bản thông tin ban đầu. Thông tin được mã hóa và giải mã bằng khóa của người dùng hoặc người nhận. Thông tin được bảo mật tuyệt đối trên đường truyền. Zedmail có thể tích hợp vào hệ thống thư điện tử doanh nghiệp và không gây bất cứ trở ngại nào. ZedMail cũng có thể tích hợp với Pushmail, được nhận và giải mã trên thiết bị di động. Người dùng bên ngoài tổ chức không có ZedMail bản quyền có thể tải “Zed!Free” miễn phí để mở email và file đính kèm và gửi lại sau đó. CISO sẽ thiết lập phương án để khôi phục hộp thư khi cần thiết. ZedMail được cài đặt trên máy người dùng và tuân theo chính sách an ninh bảo mật nội bộ; sử dụng thuật toán AES (128 đến 256 bits) và RSA (1024 đến 4096 bits), chạy trên nền tảng Microsoft Outlook, hệ điều hành Windows 7 đến 10. Bản miễn phí “Zed!Mobile” có thể chạy trên iOS và Android.
4. **CRYHOD:** Khi ổ cứng hoặc laptop bị đánh cắp hoặc thất lạc, giá trị của ổ lưu trữ không nghiêm trọng bằng giá trị thông tin lưu trữ bên trong nó. Phần mềm Cryhod mã hóa ổ cứng giúp chống trộm laptop. Người dùng có thể lựa chọn mã hóa toàn bộ các ổ đĩa hoặc từng vùng của hệ thống (C/D/E), quy trình mã hóa diễn ra ngay lập tức (on the fly) và trong suốt đối với người dùng (transparent). Trong lần mã hóa đầu tiên, nếu xảy ra sự cố như mất nguồn, tắt máy, quy trình mã hóa sẽ tự động khôi phục khi chạy lại. Cryhod tiện dụng, vận hành, giám sát theo lịch đặt GPO, tương thích và hỗ trợ phần mềm ZoneCentral. Sau khi cài đặt Cryhod, quy trình xác thực diễn ra trước khi khởi động (Pre-boot authentication), người dùng có thể sử dụng mật khẩu hoặc chứng thư, xác thực một lần SSO cùng Windows. Cryhod sử dụng thuật toán AES (128 đến 256 bits) và RSA (1024 đến 4096 bits), chạy trên hệ điều hành Windows 7 đến 10, Ubuntu và CentOS; hỗ trợ mọi loại ổ đĩa, BIOS và EFI.

5. **ZONEPOINT:** phần mềm giúp mã hóa thông tin trên MS Sharepoint, không lưu trữ thông tin mở trên máy chủ, không lưu khóa bảo mật trên hệ thống hoặc lưu chuyển trên mạng. Mọi thao tác mã hóa đều diễn ra từ máy người dùng và bằng khóa người dùng. ZonePoint bảo mật thông tin khi sử dụng dịch vụ lưu trữ trên đám mây của bên thứ 3. Quy trình mã hóa diễn ra tự động theo chính sách quy định, bất cứ tài liệu nào đưa lên Library đều được mã hóa bảo mật trước. ZonePoint hoạt động không cần cài đặt phần mềm trên máy người dùng. Thông qua Browser plug-in, phần mềm này sẽ cho phép xác thực và thực hiện mã hóa/giải mã. Sản phẩm rất phù hợp cho các doanh nghiệp muốn chia sẻ thông tin với các đối tác bên ngoài mà vẫn bảo mật thông tin. ZonePoint chạy trên Server Sharepoint 2019, 2016, 2013, Internet Explorer 7+; sử dụng thuật toán AES (128 đến 256 bits) và RSA (1024 đến 4096 bits). Ứng dụng ZoneMobile có thể chạy trên iOS và Android.
6. **ORIZON:** Phần mềm giúp bảo mật thông tin người dùng và dữ liệu chia sẻ trên đám mây. Orizon mã hóa/giải mã tự động thông tin được người dùng đồng bộ lên đám mây mà không cần bất cứ thao tác nào. Dữ liệu được liên tục mã hóa khi di chuyển và lưu trữ trên đám mây, do vậy hoàn toàn bảo mật đối với bên cung cấp dịch vụ Cloud. Orizon cũng giúp mã hóa dữ liệu phục vụ việc chia sẻ nội bộ hay với đối tác bên ngoài lưu trữ trực tuyến, đồng thời quản lý quyền đọc hiểu các thông tin này. Đối tác bên ngoài tổ chức có thể tải miễn phí Orizon Guest để làm việc trên file chia sẻ. Orizon chạy trên hệ điều hành Windows, MacOS, Linux, IOS và Android; có thể dùng mật khẩu, chứng thư hoặc token, smart card.



Khách hàng mục tiêu của giải pháp mã hóa dữ liệu Prim'X:

- Các doanh nghiệp hoạt động trong lĩnh vực ngân hàng, bảo hiểm, hàng không... sở hữu một lượng lớn thiết bị kết nối nội bộ. Dữ liệu được lưu trên máy người dùng, trên máy chủ, ổ NAS, SAN dưới dạng clear text. Chính nhân viên CNTT, hoặc nhân viên trong công ty có thể truy cập trái phép vào dữ liệu của các bộ phận nhạy cảm như kinh doanh, nhân sự & lương, tài chính kế toán, thiết kế... để đánh cắp và bán dữ liệu ra bên ngoài. Trường hợp này cần sử dụng ZoneCentral để mã hóa và phân quyền cho các cá nhân, bộ phận.
- Các doanh nghiệp có số lượng lớn laptop do các trưởng bộ phận và lãnh đạo cấp cao đang sử dụng và mang ra ngoài. Đây là những thiết bị chứa nhiều thông tin quan trọng liên quan đến chiến lược phát triển sản phẩm, đối thủ cạnh tranh... Vì vậy, họ cần cài đặt phần mềm Cryhod mã hóa các ổ chứa thông tin nhạy cảm như D, E. Nhân viên CNTT vẫn cài đặt quản lý phần mềm trên ổ C một cách bình thường. Khi máy bị đánh cắp, tin tặc không thể mở được ổ cứng do đã mã hóa.
- Các doanh nghiệp lớn có lượng nhân sự gửi email trong nội bộ và cho đối tác với nhiều thông tin nhạy cảm, nếu bị đánh cắp sẽ ảnh hưởng đến kế hoạch kinh doanh của tổ chức. Do đó, họ cần sử dụng ZedMail để mã hóa thông tin lưu chuyển qua mạng (Data in transit), cũng như file đính kèm.

- Theo xu hướng chuyển đổi số, các tài liệu bằng văn bản dần được số hóa để lưu trữ và lưu chuyển. Một cơ quan hành chính cấp tỉnh, thành phố - vốn đang lưu trữ dữ liệu công dân mang tính cá nhân và bảo mật cao - cần sử dụng phần mềm ZoneCentral và ZED để mã hóa dữ liệu khi lưu trữ và sao chép chuyển dịch, chống đánh cắp và rò rỉ.
- Các bệnh viện lớn - đang lưu trữ tất cả thông tin hồ sơ bệnh án, số bảo hiểm y tế mang tính bảo mật cao, nếu rò rỉ sẽ ảnh hưởng nghiêm trọng đến cuộc sống cá nhân, cũng gây ra nguy cơ chỉnh sửa hồ sơ bệnh án - cần cài đặt phần mềm ZoneCentral và ZED.
- Nhiều tập đoàn, công ty lớn có xu hướng thuê dịch vụ lưu trữ của bên thứ 3 trên đám mây. Thông tin không mã hóa có thể bị đánh cắp hoặc sử dụng bất hợp pháp. Do vậy, họ cần sử dụng phần mềm Orizon hoặc ZonePoint để mã hóa dữ liệu của cá nhân, tổ chức hoặc thư viện chia sẻ.
- Các tập đoàn cần bảo vệ các tài sản sở hữu trí tuệ, bí mật kinh doanh,... vd. một tập đoàn lớn đang triển khai dự án nghiên cứu một loại máy bay mới, một loại vũ khí, một sản phẩm công nghệ cao, một mẫu xe hơi thế hệ mới, một công thức hóa học... đều lưu trữ những thông tin cực kỳ quan trọng. Ngoài việc bảo vệ chống tấn công từ bên ngoài, tập đoàn này cần cài đặt các phần mềm Prim'X bảo vệ tổng thể như ZoneCentral, Zedmail, ZED, Cryhod... để bảo mật thông tin./.

(MK Group & Prim'X)



Nguồn: Internet



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