BẢN TIN NỘI BỘ

CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Xây dựng Kiến trúc Chính phủ điện tử Văn phòng Chính phủ

Mới đây, Bộ trưởng, Chủ nhiệm Văn phòng Chính phủ Mai Tiến Dũng đã phê duyệt Kế hoạch xây dựng Kiến trúc Chính phủ điện tử của Văn phòng Chính phủ giai đoạn 2020 - 2025.

Kế hoạch đề ra các nhiệm vụ: Xây dựng Đề cương Kiến trúc Chính phủ điện tử của Văn phòng Chính phủ (VPCP); sơ đồ hóa quy trình nghiệp vụ của các Vụ, Cục, đơn vị; khảo sát hiện trạng tình hình ứng dụng CNTT, xây dựng Chính phủ điện tử của VPCP; nghiên cứu bài học kinh nghiệm xây dựng Kiến trúc Chính phủ điện tử trong nước và quốc tế.

Bên cạnh đó, xây dựng Kiến trúc Chính phủ điện tử của VPCP giai đoạn 2020 - 2025 gồm: Kiến trúc nghiệp vụ; kiến trúc dữ liệu; kiến trúc ứng dụng; kiến trúc công nghệ; kiến trúc an toàn thông tin mạng; xây dựng mô hình tổng thể Kiến trúc Chính phủ điện tử của VPCP giai đoạn 2020 - 2025; đề xuất giải pháp hoàn thiện thể chế, cải tiến quy tình nghiệp vụ tại VPCP; lộ trình triển khai, mô hình quản trị, giám sát triển khai Kiến trúc Chính phủ điện tử của VPCP.

Trong đó, về xây dựng Mô hình tổng thể Kiến trúc Chính phủ điện tử của VPCP giai đoạn 2020 - 2025, xác định Mô hình tổng thể Kiến trúc Chính phủ điện tử của VPCP mô tả tổng quan các thành phần cơ bản của Kiến trúc Chính phủ điện tử, nền tảng tích hợp, chia sẻ dữ liệu dùng chung, Cổng dịch vụ công quốc gia, hệ thống thông tin báo cáo Chính phủ, hệ thống eCabinet, eConsultation và các ứng dụng CNTT, xử lý công việc trong nội bộ của VPCP, mối quan hệ giữa các thành phần và sơ đồ kết nối, liên thông với các hệ thống thông tin, cơ sở dữ liệu với các Bộ, ngành, địa phương.

Thực hiện xây dựng Kiến trúc Chính phủ điện tử của VPCP đồng bộ, thống nhất trong triển khai ứng dụng CNTT, xây dựng Chính phủ điện tử tại VPCP, phục vụ các yêu cầu cải cách hành chính, thủ tục hành chính của VPCP là góp phần vào quá trình xây dựng và phát triển Chính phủ điện tử hướng tới Chính phủ số, kinh tế số, xã hội số.

Link tham khảo: http://antoanthongtin.vn/Detail.aspx?NewsID=2f79182c-de5d-4b3a-9c55-28b530948d8d&CatID=d9e1b0f7-8656-49ef-93de-c90c7d90d4e1

2. Chỉ với vài USD đã có thể mua công cụ hack camera phòng ngủ

Công cụ hack camera phòng ngủ Amazon Ring được rao bán trên mạng với giá chỉ vài USD. Đã có nhiều vụ đột nhập liên quan tới camera an ninh này.

Công cụ hack được rao bán trên trang web ngầm, chuyên dùng để đột nhập camera Amazon có thiết lập kém an toàn. Về cơ bản, chúng cho phép kẻ xấu có thể nghe và xem hình ảnh camera phòng ngủ của bất cứ gia đình nào.

Vụ việc gần đây liên quan tới Amazon Ring đã gióng lên hồi chuông cảnh báo. Một bà mẹ tại bang Tennessee mua camera hạ giá ngày Black Friday rồi lắp trong

phòng ngủ con gái 8 tuổi. Kẻ xấu đã đột nhập vào camera rồi nói chuyện với bé gái rằng mình là ông già Noel.

Tên này thậm chí còn phát nhạc phim kinh dị qua loa camera. Người mẹ trẻ suýt ngất khi xem lại hình ảnh gây sốc này.

Tờ Motherboard cho biết kẻ xấu có thể dễ dàng mua công cụ hack camera Ring chỉ với vài USD. Phần mềm này được rao bán 8 USD.

Công cụ "Ring Video Doorbell Config" được đảm bảo có thể đột nhập vào bất cứ camera Ring nào. Một công cụ khác có chức năng tương tự là Ring.com Checker được rao bán 6 USD.

Trong khi đó, hãng sản xuất camera Ring do Amazon sở hữu bác bỏ cáo buộc đây là lỗ hổng từ nhà sản xuất. Công ty này cho biết sở dĩ tin tặc có thể dễ dàng đột nhập vào camera là do người dùng vẫn để ở thiết lập an ninh cơ bản.

Ring yêu cầu sử dụng phương pháp định danh 2 bước để nâng cao an toàn. Hãng này đang điều tra vụ việc tại Tennessee với dấu hiệu cho thấy người dùng đã sử dụng thiết lập an toàn mặc định.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra kỹ khi sử dụng camera tại nhà, áp dụng các phương pháp thay đổi mật khẩu mặc định và xác thực 2 bước để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/chi-voi-vai-usd-da-co-the-mua-cong-cu-hack-camera-phong-ngu-599785.html

3. Dùng tin nhắn giả hiệu ngân hàng để chiếm đoạt tiền

Bộ Công an vừa đưa ra cảnh báo thủ đoạn lừa đảo mới khá tinh vi giả mạo tin nhắn thương hiệu (SMS Brand Name) ngân hàng để chiếm đoạt tài sản với số tiền lớn diễn ra gần đây.

Giả mạo ngân hàng

Trước đây, tội phạm sử dụng phương thức, thủ đoạn lừa đảo phổ biến là dùng số điện thoại bất kỳ (SIM rác) để phát tán nội dung lừa đảo. Gần đây, các đối tượng lừa đảo đã thay đổi phương thức, thủ đoạn là giả mạo tin nhắn thương hiệu của các ngân hàng (NH). Nguy hiểm hơn là các tin nhắn giả mạo này lại được lưu trữ cùng thư mục với các tin nhắn thương hiệu "thật" của các NH trên điện thoại di động của người dùng. Do đó, người dân, khách hàng của các NH rất dễ nhầm tưởng đây là thông báo chính thức từ các NH hay các cơ quan hữu quan.

Cụ thể, sau khi biết được một số thông tin của khách hàng, tội phạm sẽ gửi tin nhắn với nội dung như "Trân trọng thông báo tới Quý khách! Tài khoản của bạn sẽ bị tạm ngưng dịch vụ vào ngày 1.1. Quý khách nhanh chóng đăng nhập vào http://www.***bank.top để cập nhật trực tuyến", hoặc "Kính gửi người dùng ***Bank, điểm tài khoản của bạn đã được đổi thành điều kiện quà tặng. Vui lòng đăng nhập www.***bank.vip ngay để đổi quà. Nếu quá hạn, nó sẽ không được chấp nhận"...

Trong nội dung các tin nhắn luôn kèm đường dẫn đến các trang web giả mạo do các đối tượng quản lý (các trang web này có tên gần giống với các trang web chính thức của NH) nên người dùng dễ lầm tưởng, mất cảnh giác. Khi người dùng truy cập vào đường dẫn trong nội dung tin nhắn, hệ thống sẽ tự động hiển thị một trang web có giao diện, logo tương tự các website chính thức của NH và được yêu cầu điền các thông tin như tên đăng nhập, mật khẩu, mã OTP... Khi có được các thông tin, các đối tượng sẽ kiểm soát được tài khoản chuyển tiền trực tuyến của khách hàng và thực hiện được các hành vi như: chuyển khoản, mở thấu chi, topup thẻ tín dụng, đăng ký vay online...

Một hình thức giả mạo NH lừa đảo khác cũng mới xuất hiện gần đây là bán hồ sơ vay vốn giải ngân. Ngân hàng TMCP Tiên Phong (TPBank) vừa qua đã phải cảnh báo trường hợp giả mạo NH trên mạng xã hội với Facebook có tên "TPBank - Bán Hồ Sơ Vay Vốn Giải Ngân Trong Ngày" thông báo bán hồ sơ giải ngân duyệt sẵn có thu phí của TPBank. TPBank khẳng định Facebook này không thuộc quản lý của NH, không thể đại diện cho NH để tư vấn cho khách hàng về các sản phẩm dịch vụ TPBank cung cấp. Bên cạnh đó, việc mua bán này hoàn toàn trái với các quy định hiện hành của nhà băng.

Theo quy trình hiện tại, khách hàng có nhu cầu vay vốn tại TPBank cần làm việc trực tiếp với cán bộ bán hàng của NH ở các đơn vị kinh doanh để được tư vấn về sản phẩm dịch vụ, đồng thời phải trải qua quá trình thẩm định, xét duyệt hồ sơ nghiêm ngặt từ phía TPBank. Chỉ khi khách hàng đáp ứng đủ điều kiện theo quy định mới được giải ngân.

Chèn tin nhắn giả mạo

Ông Vũ Ngọc Sơn, Phó chủ tịch Bkav, cho biết bản chất quá trình gửi 1 SMS Brand Name được thực hiện một phần qua internet, nên không loại trừ khả năng tội phạm đã lợi dụng 1 khâu nào đó trong quá trình diễn ra trên internet này để gửi mạo danh. Điều này cũng giống như việc mạo danh email vốn đã rất phổ biến trước đây. Sau khi đã mạo danh được thì việc tin nhắn giả mạo được chèn vào thư mục của SMS Brand Name mà các đơn vị đang triển khai hoàn toàn có thể xảy ra ở góc độ kỹ thuật.

Liên lạc với nhà mạng Vinaphone đề nghị đăng ký dịch vụ SMS Brand Name và đặt vấn đề nhà mạng có cho đăng ký trùng với một đơn vị khác mà ghi khác đi là chữ viết hoa hay không viết hoa, nhân viên nhà mạng này cho hay việc đăng ký tên có phân biệt chữ hoa và chữ thường, nên trong trường hợp tên đó chưa ai đăng ký thì vẫn được. Riêng việc tội phạm đi đăng ký SMS Brand Name với tên gọi na ná của doanh nghiệp để thực hiện lừa đảo, theo ông Sơn: "Để đăng ký SMS Brand Name có một quy trình và nhiều thủ tục, mang tính định danh cao nên tội phạm sẽ không thực hiện mà có thể khai thác ở góc độ nào đó trong quá trình thực hiện SMS Brand Name".

Bộ Công an đánh giá các đối tượng đã lừa đảo qua hình thức giả mạo SMS Brand Name chiếm đoạt tài sản của nhiều khách hàng với số tiền rất lớn, xảy ra tại nhiều địa phương trong cả nước. Với phương thức phát tán tin nhắn Brand Name giả

mạo NH, khách hàng rất khó phân biệt được thật giả, không những bị thiệt hại về tài sản mà còn gây ảnh hưởng đến uy tín của các NH nói riêng và cả hệ thống thanh toán nói chung. Thủ đoạn này sẽ đặc biệt nguy hiểm khi bị các đối tượng xấu lợi dụng để giả mạo các thông báo chính thức của cơ quan nhà nước, gửi tin nhắn xuyên tạc, không đúng sự thật đến người dân.

Dịp cuối năm, khi khối lượng giao dịch trong tài khoản NH là rất lớn, cũng là thời điểm các đối tượng phạm tội gia tăng hoạt động. Do đó Bộ Công an khuyến cáo người dân khi nhận được những tin nhắn như trên cần kiểm tra kỹ nội dung nhận được kể cả các tin nhắn thương hiệu từ NH, không vội vã trả lời hay thực hiện theo nội dung trong tin nhắn. Website chính thức của các tổ chức, doanh nghiệp sẽ được đăng ký với các cơ quan có thẩm quyền và được đánh dấu an toàn bằng hình ổ khóa bên cạnh tên miền website (giao thức https)...

Hầu hết các NH đều khuyến cáo khách hàng không nên truy cập những đường link lạ từ các tin nhắn, thư điện tử hay yêu cầu của ai, kể cả nhân viên NH yêu cầu cung cấp số tài khoản, mật khẩu, OTP.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra kỹ nội dung khi nhận được các tin nhắn có liên quan đến tài khoản ngân hàng, đặc biệt khi có những yêu cầu liên quan đến cung cấp số tài khoản, mật khẩu hay OTP để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/dung-tin-nhan-gia-hieu-ngan-hang-de-chiem-doat-tien.13057/

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Wordpress	CVE-2019-19133 CVE-2019-19589	Nhóm 02 lỗ hổng trên một số thành phần của Wordpress (CSSHere plugin through 4.0.3) cho phép đối tượng tấn công thu thập thông tin.	Đã có thông tin xác nhận và bản vá.
2	Linux	CVE-2019-19602 CVE-2019-19462 CVE-2019-19377 …	Nhóm 04 lỗ hổng trên hệ điều hành Linux (kernel 5.0.21) cho phép đối tượng tấn công tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
3	Huawei	CVE-2019-5269 CVE-2019-5210 CVE-2019-5225 …	Nhóm 16 lỗ hổng trên thiết bị Huawei (home routers, Nova 5iPro, P30, Mate 20, P30 Pro smartphones…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã tùy ý, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
4	Android	CVE-2019-2217 CVE-2019-9464 CVE-2019-2223 …	Nhóm 34 lỗ hổng trên hệ điều hành Android (Androi-8.1/8.0, Android-10…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh từ xa.	Chưa có thông tin xác nhận và bản vá
5	D-link	CVE-2019-19598 CVE-2019-19597	Nhóm 02 lỗ hổng trên thiết bị Dlink (DAP-1860 trước phiên bản v1.04b03) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
6	Apache	CVE-2019-17554 CVE-2019-17555 CVE-2019-17556	Nhóm 03 lỗ hổng trên sản phẩm của Apache (Apache Olingo) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	vptdjfz2w.ru
5	xjpakmdcfuqe.biz
6	xjpakmdcfuqe.com
7	xjpakmdcfuqe.in

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:
   - Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
   - Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.