TÀI LIỆU

NHỮNG CÁNH CỬA BỎ NGỎ

NGHIÊN CỨU CHO THẤY MÁY IN CÓ THỂ DỄ DÀNG BỊ TẤN CÔNG MẠNG.

Trong khi đội ngũ CNTT tập trung vào các thiết bị đầu cuối khác, vấn đề bảo mật cho các máy in của doanh nghiệp vẫn còn đang bỏ ngỏ.

Máy in đang trở thành mục tiêu dễ dàng: Quá nhiều máy in kết nối mạng mà không có chính sách hạn chế và không được bảo mật an toàn.

Tuy nhiên mối đe dọa dành cho máy in là có thật và không nên xem thường. Các máy in doanh nghiệp ngày nay đã phát triển thành những thiết bị kết nối mạng mạnh mẽ, và tồn tại những lỗ hổng tương tự như bất kỳ thiết bị đầu cuối nào khác trong hệ thống mạng của bạn. Những điểm truy cập không được bảo mật này tiềm ẩn nguy cơ thật sự về việc bị tấn công mạng; chúng cung cấp khả năng truy cập vào các dữ liệu tài chính và nhạy cảm của công ty bạn, dẫn tới những hậu quả khó lường về kinh doanh.

Mặc dù vậy, một khảo sát gần đây của Spicework đối với hơn 300 nhà quản lý CNTT doanh nghiệp cho thấy chỉ có 16% nghĩ rằng máy in tiềm ẩn rủi ro cao về lỗ hổng bảo mật, thấp hơn đáng kể so với máy tính để bàn, máy tính cá nhân và các thiết bị di động.[1] Nhận thức này đã làm ảnh hưởng đến cách thức tiếp cận vấn đề an ninh mạng của đội ngũ nhân viên CNTT. Chỉ có gần 3/5 tổ chức có các biện pháp thực hành bảo mật thích hợp dành cho máy in, tỷ lệ này thấp hơn đáng kể so với tỷ lệ dành cho các thiết bị đầu cuối khác – và điều này khiến máy in trở nên dễ bị tấn công, trong khi có những giải pháp dễ dàng để có thể bảo vệ điểm truy cập đặc biệt này.

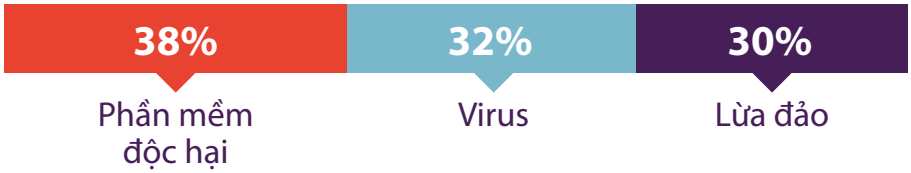
Tài liệu này đưa ra các dữ liệu về bảo mật máy in dựa trên khảo sát Spiceworks, ảnh hưởng của các lỗ hổng bảo mật, và một số tính năng bảo mật được tích hợp trong máy in hiện đại được thiết kế để bảo vệ chống lại tấn công mạng.

CHỈ 16% NGƯỜI THAM GIA KHẢO SÁT CHO RẰNG MÁY IN ĐANG ĐỨNG TRƯỚC MỐI ĐE DỌA VỀ LỖ HỔNG BẢO MẬT.[1]

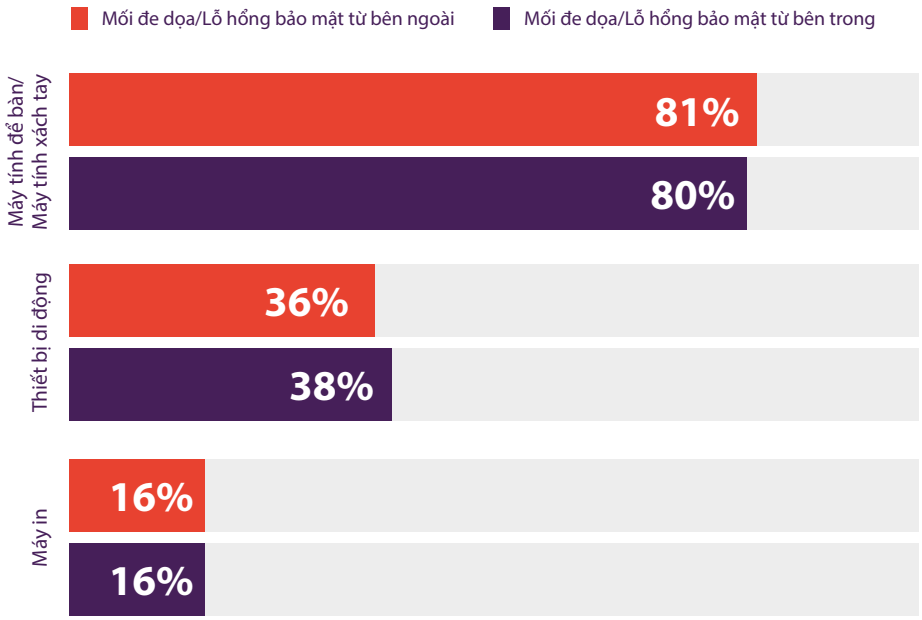
CÁNH CỬA BỎ NGỎ CHO NHỮNG CUỘC TẤN CÔNG

Trong khảo sát của Spiceworks, 74% số người được hỏi (con số thực tế) cho biết tổ chức của họ đã gặp ít nhất một loại nguy cơ hay tấn công bảo mật CNTT từ bên ngoài trong năm qua. Và 70% (thực tế) đã từng gặp nguy cơ hay lỗ hổng bảo mật CNTT nội bộ, nguyên nhân phổ biến nhất là do lỗi người dùng, sử dụng các thiết bị cá nhân cho mục đích công việc hay nhân viên sử dụng mạng tại nhà, mạng công cộng cho mục đích công việc.[1]

NHỮNG NGUY CƠ CAO NHẤT VỀ MỐI ĐE DỌA/LỖ HỔNG BẢO MẬT CNTT TỪ BÊN NGOÀI



Các mối đe dọa xâm nhập hàng đầu chủ yếu qua con đường máy tính để bàn và máy tính cá nhân, trong khi một số khác xâm nhập qua các thiết bị di động và máy in.[1] (16% xâm nhập thông qua máy in là con số cao hơn đáng kể so với tỷ lệ 4% theo nghiên cứu tương tự của Spiceworks vào năm 2014). Điều này cũng có thể do số lượng tấn công thông qua máy in bị đánh giá thấp, do máy in không được giám sát chặt chẽ như máy tính cá nhân và thiết bị di động.



CHÚNG TA ĐANG BỎ QUA MÁY IN

Bất kể trong tình huống nào, khảo sát Spiceworks chỉ ra rằng vấn đề bảo mật máy in luôn bị xem nhẹ.

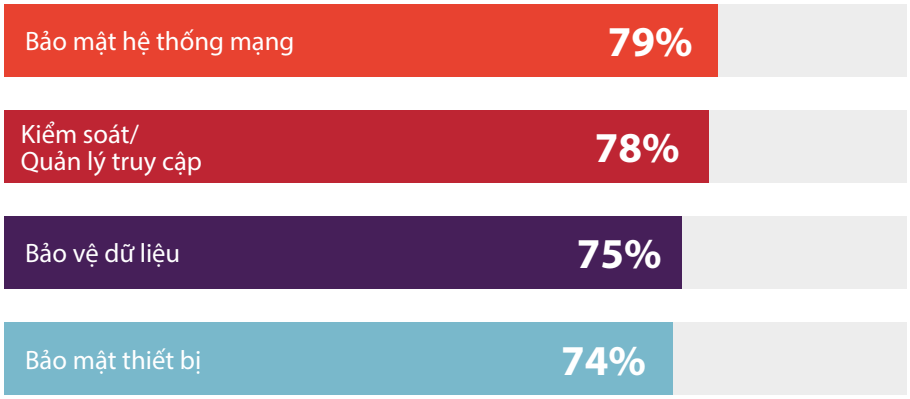
Các tổ chức thường nhận thức sâu sắc về tầm quan trọng của hệ thống mạng, các thiết bị đầu cuối và vấn đề bảo mật dữ liệu. Trong thực tế, hơn ba phần tư số người được hỏi áp dụng các biện pháp an minh mạng, kiểm soát/quản lý việc truy cập, bảo vệ dữ liệu hoặc bảo mật các thiết bị đầu cuối – hay kết hợp những biện pháp kể trên.[1]

Nhưng những biện pháp nói trên được triển khai ít hơn rất nhiều cho hệ thống máy in. Trong khi 83% người tham gia khảo sát áp dụng biện pháp an ninh mạng trên máy tính để bàn/máy tính xách tay và 55% trên thiết bị di động, chỉ có 41% thực hiện điều tương tự trên máy in.[1]

Sự chênh lệch đó thậm chí còn lớn hơn đối với việc bảo mật thiết bị đầu cuối:

Thêm vào đó, thậm chí chưa đến một phần ba (28%) số người tham gia khảo sát triển khai các chứng nhận bảo mật dành cho máy in, trái ngược với con số 79% dành cho máy tính cá nhân và 54% cho các thiết bị di động.[1]

CÁC BIỆN PHÁP BẢO MẬT THIẾT BỊ ĐẦU CUỐI PHỔ BIẾN NHẤT



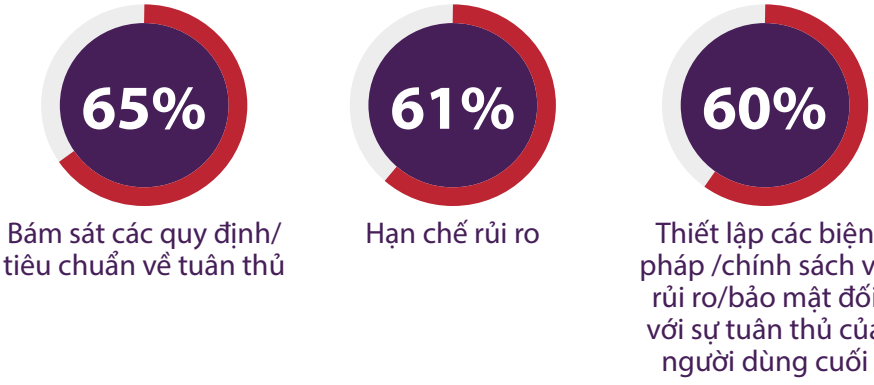
Trong số các biện pháp bảo vệ áp dụng trên các thiết bị đầu cuối nói chung, biện pháp bảo mật được áp dụng nhiều nhất cho máy in là bảo mật tài liệu, bảo mật hệ thống mạng và kiểm soát truy cập, nhưng chưa đến một nửa số người được hỏi cho biết tổ chức của họ không áp dụng bất kỳ biện pháp nào trong số đó trên máy in của tổ chức.[1]

Một số công ty có các biện pháp bảo mật dành riêng cho máy in, nhưng ngay cả ở các công ty như vậy, các biện pháp này cũng có sự khác biệt rất lớn. Chỉ hơn 40% các tổ chức cho triển khai xác thực người dùng, và chưa tới 40% sử dụng mật khẩu quản trị viên cho giao diện cấu hình web.[1] Để có được tấm chắn bảo mật mạnh mẽ, mỗi tổ chức nên sử dụng kết hợp tất cả các phương pháp này – và còn hơn thế nữa.

CÁC BIỆN PHÁP BẢO MẬT DÀNH RIÊNG CHO MÁY IN

Khi nói tới việc tuân thủ và các biện pháp kiểm tra thiết bị đầu cuối, kiểm soát bảo mật máy in thường xếp sau hầu hết mọi thiết bị đầu cuối khác. Gần 90% các tổ chức đã cho triển khai chính sách bảo mật thông tin, tuy nhiên những chính sách này thường không xét tới máy in. Ví dụ như, trong khi 57% số người tham gia khảo sát cho biết có triển khai bảo vệ chống phần mềm độc hại trên máy tính cá nhân, chỉ 17% cho biết có triển khai việc này trên máy in.[1]

GẦN 9 TRÊN 10 CHUYÊN GIA CNTT NHẬN ĐỊNH RẰNG TỔ CHỨC CỦA HỌ CÓ MỘT CHÍNH SÁCH BẢO MẬT THÔNG TIN THÍCH HỢP, VỚI NHỮNG LÝ DO NHƯ SAU:



Rõ ràng, các tổ chức chưa nhìn nhận nghiêm túc về vấn đề bảo mật dành cho máy in – mà đáng lẽ ra họ cần làm vậy.

"Nhiều máy in vẫn còn dùng mật khẩu mặc định hoặc thậm chí không hề dùng mật khẩu nào, hay có tới mười máy cùng dùng chung mật khẩu," Michael Howard, giám đốc cố vấn bảo mật cho HP chia sẻ trên tạp chí Computerworld hồi tháng 6. "Máy in không sử dụng biện pháp bảo vệ mật khẩu là mỏ vàng cho tin tặc. Một trong những lỗ hổng ta thường xuyên chứng kiến là việc tấn công man-in-the-middle (nghe lén trên mạng), khi đó chúng chiếm quyền sử dụng một máy in và chuyển [tài liệu đi] đến một máy tính cá nhân trước khi tài liệu được in ra. Chúng có thể thấy mọi thứ mà một vị CEO đang in."[2]

ẢNH HƯỞNG TIỀM ẨN CỦA VIỆC XÂM NHẬP MÁY IN

Theo Bogdan Botezatu - nhà phân tích mối đe dọa điện tử cấp cao tại Bitdefender, máy in là lỗ hổng bảo mật tiềm ẩn không nên xem nhẹ. "Chúng tôi thực hiện nhiều phép đo từ xa trong các thí nghiệm đánh giá lỗ hổng. Bộ định tuyến hiện không còn là thiết bị dễ xâm nhập nhất trên Internet. Giờ đây, đó chính là máy in."[3]

Lỗ hổng này có thể gây ra những hậu quả to lớn cho một doanh nghiệp. Chỉ cần một máy in không an toàn cũng có thể khiến toàn bộ các thiết bị kết nối trong hệ thống mạng của bạn bị tấn công, trao cho tin tặc khả năng làm gián điệp trên các thiết bị được kết nối mạng của doanh nghiệp – và gây ảnh hưởng tới bảo mật toàn hệ thống mạng.

Chúng ta đã chứng kiến những hậu quả của các lỗ hổng bảo mật. Trong khảo sát của Spiceworks, những người tham gia khảo sát cho biết năm ảnh hưởng lớn nhất của một lỗ hổng bảo mật là:[1]

1. Tăng số lượng cuộc gọi cũng như thời gian hỗ trợ

2. Giảm năng suất/ hiệu quả

3. Tăng thời gian hệ thống ngừng hoạt động

4. Tăng thời gian các cuộc gọi hỗ trợ

5. Tăng cường thực thi chính sách người dùng cuối

Nhưng một lỗ hổng về máy in thậm chí còn có thể trầm trọng hơn thế, nhất là khi bạn sử dụng một máy in đa năng có khả năng lưu trữ dữ liệu in điện tử. Các lệnh in được lưu trữ trong bộ nhớ đệm của máy in tạo điều

kiện cho tin tặc có quyền truy cập vào các thông tin nhạy cảm của cá nhân hoặc doanh nghiệp.

Thậm chí còn đáng lo ngại hơn, tin tặc có thể truy cập sâu rộng hơn vào hệ thống mạng công ty thông qua một máy in không bảo mật, đánh cắp thông tin như số anh sinh xã hội, thông tin tài chính hay biên bản và tài liệu nội bộ. Thông tin bị đánh cắp này có thể gây ảnh hưởng không chỉ tới nhân viên theo phương diện cá nhân mà còn được đối thủ cạnh tranh sử dụng hoặc gây ra những thiệt hại nghiêm trọng cho uy tín của công ty.

GIẢI PHÁP DỄ DÀNG: TÍCH HỢP TÍNH NĂNG BẢO MẬT

Rõ ràng, các doanh nghiệp cần giải quyết vấn đề bảo mật ngay cả với hệ thống máy in. Một số máy in dùng trong doanh nghiệp hiện đại ngày nay có tính năng bảo mật được tích hợp và dễ dàng sử dụng nhằm chống lại các mối đe dọa với máy in. Những biện pháp này bao gồm:

- Tự động phát hiện tấn công, bảo vệ và hồi phục
- Theo dõi việc sử dụng để ngăn chặn sử dụng trái phép
- Các tùy chọn truy cập đơn giản như mã PIN hoặc thẻ thông minh
- Một đầu đọc thẻ từ giúp người sử dụng nhanh chóng xác thực và in một cách an toàn tại máy in khi sử dụng thẻ nhận dạng
- In mã hóa an toàn các tài liệu có nội dung nhạy cảm

Khi xem xét lựa chọn mua máy in mới, cho dù là máy bàn hay máy in đa năng, hãy tìm hiểu về các biện pháp bảo vệ bảo mật tích hợp – và chắc chắn kích hoạt các biện pháp này. Với những tính năng đơn giản, dành riêng cho máy in như vậy, sẽ không còn những lỗ hổng bảo mật thông qua máy in; xét cho cùng thì với Mạng lưới thiết bị kết nối Internet (Internet of Things), còn vô số điểm truy cập đáng lo khác – **và không nên để máy in là một trong số đó.**

TÌM KIẾM CÁC MÁY IN BẢO MẬT KHÁC?
TÌM HIỂU THÊM ›

Nguồn:

[1] Nghiên cứu của Spiceworks đối với 309 người ra quyết định về CNTT tại Bắc Mĩ, Khu vực Châu Âu, Trung Đông và Châu Phi và Khu vực Châu Á-Thái Bình Dương, thay mặt HP thực hiện, tháng 11/2016.

[2] "Bảo mật máy in: Dữ liệu của công ty bạn có thực sự được an toàn?" *Computerworld*, ngày 1 tháng 6 năm 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Máy in hiện nay là thiết bị kém được bảo mật nhất trên mạng Internet", *The Register*, ngày 8 tháng 9 năm 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/