Bảo vệ

Yếu tố con người

Paul Kearney

IT Governance Publishing

Bảo vệ

Yếu tố con người

Bảo vệ

Yếu tố con người

PAUL KEARNEY

IT Governance Publishing

Xuất bản Quản trị CNTT
Công Ty TNHH Quản Trị CNTT
Đơn vị 3, Tòa án Clive
Lối đi của Bartholomew
Khu thương mại Cambridgeshire
Ely
Cambridgeshire
CB7 4EH
Vương quốc Anh

www.itgovernance.co.uk

Được xuất bản lần đầu tại Vương quốc Anh vào năm 2010 bởi Nhà xuất bản Quản trị CNTT.

ISBN: 978-1-84928-064-8

LỜI TỰA

An ninh thông tin – công ty, thương mại và cá nhân – đang bị đe dọa lớn hơn bao giờ hết.

Lý do là một trong những đơn giản. Tất cả chúng ta đều bị cuốn vào một cuộc 'chạy đua vũ trang' giữa một bên là đội quân du kích gồm những tên trộm, tin tặc và những kẻ phá bĩnh, và bên kia là một lực lượng quyết liệt không kém gồm những 'người tốt'. Khi cuộc sống của chúng ta ngày càng trở nên trực tuyến và kỹ thuật số, tiền cược ngày càng cao hơn.

Vì vậy, những người tốt điều khiển các phòng thủ là ai?

Thật hấp dẫn khi chỉ tập trung vào các chuyên gia bảo mật. Xét cho cùng, họ là những người hiểu rõ nhất về những gì đang bị đe dọa, các kỹ thuật mà phe đối lập sử dụng để thực hiện các cuộc tấn công cũng như cách bảo vệ cơ sở và hệ thống CNTT trước mối đe dọa.

Nhưng quan điểm này sẽ đơn giản. Cho dù họ có tay nghề cao đến đâu, các chuyên gia bảo mật cũng không thể hy vọng bảo vệ các tổ chức bằng cách tự mình làm việc. Lấy bảo mật CNTT làm ví dụ. Ngày nay, bạn ít nghe về các trường hợp tin tặc có thể truy cập vào hệ thống CNTT của tổ chức và đánh cắp thông tin, và vì lý do chính đáng. Các nhóm bảo mật CNTT đã trở nên rất giỏi trong công việc của họ. Nhưng những câu chuyện về những người bỏ máy tính xách tay trên tàu hỏa, tài liệu bí mật được trưng bày ở những nơi công cộng, v.v., rất nhiều.

Như hướng dẫn bỏ túi này đã làm rõ, để bảo vệ tổ chức hiệu quả nhất có thể, bạn cần tập trung vào ba điều: con người, quy trình và

công nghệ. Bất kể bạn đầu tư bao nhiêu vào các quy trình và công nghệ bảo mật, sẽ là lãng phí nếu nhân viên của bạn không hiểu các vấn đề đang bị đe dọa, cách họ có thể giúp bảo vệ tổ chức của bạn cũng như cách sử dụng các quy trình và công nghệ liên quan.

Ray Stanton
Giám đốc điều hành toàn cầu của Kinh doanh liên tục,
An ninh và Quản trị, BT Global Services

LỜI NÓI ĐẦU

Người ta thường cho rằng những người làm việc trong các tổ chức là nguyên nhân của hầu hết các vấn đề về bảo mật thông tin. Họ viết mật khẩu trên Post it® Notes, để máy tính xách tay trên tàu hỏa, nói về những chủ đề nhạy cảm ở nơi công cộng, v.v. Tại sao họ không thể chỉ tuân theo các chính sách?

Vấn đề với quan điểm này là nó quá đơn giản.
Vâng, mọi người gây ra vấn đề, nhưng điều này thường không cố ý. Hãy xem xét kỹ bất kỳ sự cố nào, và thường xuyên hơn không, bạn sẽ thấy ai đó đang cố gắng thực hiện công việc tốt nhất có thể mà họ có thể, nhưng lại được đào tạo kém về cách sử dụng các công cụ và quy trình bảo mật, đã bị xúc phạm. bởi mâu thuẫn ưu tiên, hoặc đơn giản là không biết hành động của mình có thể gây ra vấn đề.

Trên thực tế, có ba điều quan trọng – con người, quy trình và công nghệ. Nếu các tổ chức muốn giữ an toàn cho các hệ thống CNTT mà họ sở hữu và thông tin họ nắm giữ, thì họ phải giải quyết cả ba vấn đề này. Không phải là các thành phần độc lập, mà là một sự kết hợp hỗ trợ lẫn nhau.

Hướng dẫn bỏ túi này xem xét những thách thức mà điều này có thể gây ra, hậu quả của việc không đáp ứng được những thách thức đó và quan trọng nhất là các bước mà các tổ chức có thể thực hiện để khiến bản thân và thông tin của họ trở nên an toàn hơn.

Tôi hy vọng bạn thấy nó hữu dụng.

Paul Kearney

GIỚI THIỆU VỀ TÁC GIẢ

Paul Kearney là Trưởng nhóm nghiên cứu bảo mật tại Security Futures Practice, BT Innovate and Design.

Ông gia nhập BT vào năm 1997, trước đó đã từng làm việc trong ngành công nghiệp điện tử cá nhân và hàng không vũ trụ quốc phòng.

Paul đã làm việc trong lĩnh vực nghiên cứu bảo mật thông tin từ năm 2001. Là Chuyên gia Bảo mật Hệ thống Thông tin được Chứng nhận (CISSP) và là Thành viên của Viện Chuyên gia Bảo mật Thông tin (MInstISP), ông là đồng tác giả của sách trắng, 'Lỗ hổng của Con người trong Bảo mật Systems', được xuất bản năm 2007 bởi Mạng chuyển giao kiến thức an ninh mạng. Mạng này là một trong số các cơ quan do chính phủ tài trợ được thành lập để giữ cho Vương quốc Anh đi đầu trong cuộc cách mạng kỹ thuật số, bằng cách tạo và chia sẻ kiến thức chuyên môn.

Paul lần lượt lấy bằng Cử nhân và Tiến sĩ vật lý lý thuyết tại Đại học Liverpool và Durham. Anh ấy làm việc tại Trung tâm Công nghệ Adastral Park của BT, gần Ipswich ở Suffolk.

NỘI DUNG

GIỚI THIỆU

'Mọi người đôi khi phạm sai lầm và làm những việc mà họ không nên làm. Rốt cuộc, họ chỉ là con người. Các tổ chức công nghệ, truyền thông và viễn thông nên tập trung nhiều hơn vào khía cạnh con người của bảo mật, đặc biệt là các lỗ hổng nội bộ.'

Deloitte, 20101

Thiệt hại về uy tín và hình ảnh thương hiệu, mất doanh thu và cơ sở khách hàng, rò rỉ quyền sở hữu trí tuệ và thông tin thương mại cho đối thủ cạnh tranh, phạt tiền và truy tố hình sự, là một trong những hậu quả đối với các tổ chức vi phạm an ninh.

Những tiến bộ trong công nghệ thông tin nhân lên mức độ vi phạm tiềm năng và tốc độ lan truyền của chúng. Đồng thời, tội phạm mạng đã phát triển thành các tổ chức và chuyên nghiệp hơn, được phục vụ bởi nền kinh tế đen trong các bộ công cụ phần mềm độc hại và thông tin bị đánh cắp. Mọi doanh nghiệp cần nhận thức được những rủi ro mà mình gặp phải, doanh nghiệp phải liên tục xem xét và làm mới các biện pháp bảo mật của mình, đồng thời luôn cảnh giác trong trường hợp các biện pháp đó không thành công.

Theo một cách nào đó, điều này không có gì mới. Trên chiến trường thời trung cổ, các hiệp sĩ tự bảo vệ mình bằng áo giáp làm từ các tấm kim loại có khớp nối, dây xích và đệm. Mỗi tấm có mục đích của nó và

---

[1] 'Nghiên cứu An ninh Toàn cầu TMT năm 2010: Những phát hiện chính', Deloitte, 2010, www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/2010_TMT_Global_Security_study.pdf

được định hình phù hợp, nhưng cũng phải kết nối linh hoạt với các nước láng giềng. Các thành phần của áo giáp nói chung phải bao phủ tất cả các vùng chiến lược của cơ thể – đầu, ngực, cánh tay, v.v. – nhưng vẫn phải cho phép hiệp sĩ hoạt động như một cỗ máy chiến đấu.

Bất kỳ lỗ hổng nào cũng sẽ nhanh chóng bị khai thác bởi các đối thủ thấp hơn, trang bị kém hơn, nhưng đông hơn và nhanh nhẹn hơn. Do đó, thiết kế của áo giáp chắc chắn là một sự thỏa hiệp, giữa một mặt là tối đa hóa sức mạnh và độ che phủ hoàn chỉnh, mặt khác là giảm thiểu tác động đến sự dễ dàng di chuyển, tầm nhìn và giao tiếp. Các vấn đề như chi phí và sự phô trương của cải và địa vị cũng đóng vai trò quan trọng.

Giống như hiệp sĩ ngày xưa, tổ chức hiện đại dựa vào sự tương tác hài hòa của các yếu tố không giống nhau để bảo vệ, thường được nhóm lại dưới các tiêu đề 'con người', 'quy trình' và 'công nghệ'. Một đối thủ đang tìm cách xâm phạm bảo mật thông tin của tổ chức, đương nhiên sẽ chọn con đường dễ dàng nhất và điều này thường là bằng cách thao túng mọi người hoặc khai thác lỗi của họ. Do đó, thật hấp dẫn khi kết luận rằng mọi người 'không tốt cho an ninh' và rằng các vấn đề nên được đưa ra khỏi tầm tay của họ thông qua tự động hóa hoặc kỷ luật cứng nhắc. Nhưng đây sẽ là một sai lầm. Nhìn chung, nhân viên không cố ý vi phạm bảo mật – việc kẻ tấn công có thể dễ dàng khai thác chúng thường là kết quả của công nghệ và quy trình được thiết kế kém hoặc thiếu đào tạo thích hợp.

Nhiều chuyên gia bảo mật (bao gồm cả tôi) là các nhà công nghệ và chúng tôi coi trọng

người dùng như một tội ác cần thiết, những người mà công nghệ phải được bảo vệ. Quan điểm ngược lại - sai lầm là do con người, nhưng để làm hỏng mọi thứ một cách triệt để thì cần đến một chiếc máy tính – cũng phổ biến không kém và sai lầm không kém. Vấn đề thực sự không phải là một bên tốt và bên kia xấu, mà là phần cứng và con người có những đặc điểm rất khác nhau. Trong khi máy tính sẽ thực hiện cùng một nhiệm vụ một cách đáng tin cậy, ngày này qua ngày khác, bất kể kết quả có hợp lý hay không, con người sẽ phạm sai lầm, diễn giải các hướng dẫn khác nhau tùy thuộc vào tâm trạng và áp dụng lẽ thường của họ cho điều tốt hay điều xấu. Do đó, không có gì đáng ngạc nhiên khi nhiều vấn đề bảo mật quan trọng nhất phát sinh ở giao diện giữa con người và công nghệ.

Yếu tố thứ ba của một tổ chức là quy trình. Nếu chúng ta ví một tổ chức với một hệ thống máy tính, thì các quy trình kinh doanh về cơ bản là các chương trình quy định những gì nó làm. Các chương trình này 'thực thi' trên hai loại phần cứng khác nhau – con người và CNTT – mỗi thứ đều có điểm mạnh và điểm yếu. Việc tự động hóa các phần của quy trình kinh doanh có thể mang lại khả năng dự đoán và hiệu quả, nhưng đòi hỏi nó phải được chỉ định một cách chi tiết theo quy định. Nếu nhà thiết kế quy trình bỏ qua các lỗ hổng bảo mật, khả năng dự đoán của hệ thống CNTT sẽ trở thành một điểm yếu mà kẻ tấn công có thể khai thác – một điểm yếu có thể bị khai thác nhiều lần chỉ trong một khoảng thời gian ngắn.

Mặt khác, mọi người có thể giải thích các hướng dẫn. Đây đồng thời là một điểm mạnh và một điểm yếu. Một người có thể đối phó với những hướng dẫn được diễn đạt kém và điều chỉnh những hướng dẫn họ được đưa ra cho phù hợp với hoàn cảnh mà họ thực sự phải đối mặt.

Hơn nữa, nhân viên có thể (và làm) phát hiện các vấn đề và hoạt động đáng ngờ, áp dụng lẽ thường và sử dụng sáng kiến của họ để can thiệp hoặc kêu gọi hỗ trợ. Thật không may, họ cũng sẽ điều chỉnh, hoặc thực sự bỏ qua các hướng dẫn hoàn toàn, chính xác và được diễn đạt chính xác, nếu chúng có vẻ không có ý nghĩa trong lần đọc đầu tiên hoặc gây bất tiện. Tuy nhiên, từ quan điểm của kẻ tấn công, điều quan trọng về chúng là chúng có thể bị thao túng.

Trọng tâm của hướng dẫn bỏ túi này là giải quyết các điểm yếu của con người – tức là các điểm yếu trong bảo mật của tổ chức do các đặc điểm và hành vi của con người. Tuy nhiên, vì ba yếu tố tổ chức phụ thuộc lẫn nhau nên chúng ta cũng cần xem xét tác động của các quy trình và công nghệ đối với sự đóng góp của mọi người đối với an ninh.

Phương pháp mà tôi đề xuất và trình bày trong tài liệu hướng dẫn bỏ túi này có ba nguyên tắc chính:

- Cho phép mọi người đóng góp tích cực cho an ninh thông qua các chiến dịch nâng cao nhận thức, giáo dục, động lực và trao quyền.
- Thiết kế các quy trình, chính sách khuyến khích và bảo mật để giảm thiểu xung đột lợi ích và giúp mọi người dễ dàng hành xử an toàn.
- Thiết kế các giải pháp kỹ thuật với các giao diện dễ sử dụng và cung cấp cho người dùng các mô hình trực quan về chức năng của chúng.

Trong chương đầu tiên, tôi sẽ thảo luận về một số phẩm chất của con người có thể dẫn đến điểm yếu, từ quan điểm bảo mật, mặc dù nhiều trong số này cũng có mặt tích cực.

CHƯƠNG 1: BẤT NGỜ

'Lỗi của con người được cho là điểm yếu {bảo mật} lớn nhất trong năm nay (86%), tiếp theo là công nghệ (63%) ... Trừ khi rô-bốt thay thế lực lượng lao động của con người (không chắc trong đời có ai đọc báo cáo này), lỗi của con người là một vấn đề mà các công ty sẽ tiếp tục giải quyết.'

Deloitte, 20092

Hãy xem xét một số cách mà bản chất con người có thể góp phần vào các vi phạm an ninh, bắt đầu từ sự bất cẩn.

Hầu như không có tuần nào trôi qua mà không có báo cáo về việc máy tính xách tay hoặc thẻ nhớ USB chứa thông tin nhạy cảm bị bỏ quên trên tàu hỏa hoặc bị đánh cắp khi để ở nơi dễ thấy trên ghế sau ô tô. Thiết bị điện tử hiện đại có tính di động cao và có thể chứa lượng dữ liệu đáng kinh ngạc. Nhân viên được khuyến khích tích cực tận dụng tính di động này, làm việc khi đang di chuyển và ở nhà, vì vậy họ khó có thể bị chỉ trích khi họ làm việc. Chúng tôi cũng không chỉ nói về máy tính xách tay. Thật dễ dàng để đánh giá thấp khối lượng và giá trị của thông tin được lưu trữ trên điện thoại thông minh và các thiết bị khác được sử dụng trong cả công việc kinh doanh và cuộc sống cá nhân của chúng ta.

---

2 'Bảo vệ những gì quan trọng – Khảo sát An ninh Toàn cầu Hàng năm lần thứ 6', Deloitte, 2009, www.deloitte.com/view/en_CZ/cz/industries/fsi/article/66b7bf2733101210VgnVCM100000ba42f00aRCRD.htm.

1: Bất cẩn

Trước đây, mọi người đi họp sẽ chỉ đóng gói cặp tài liệu của họ với những giấy tờ họ cần trong ngày. Mọi thứ khác đều bị bỏ lại phía sau.
Giờ đây, chúng tôi có thể mang theo mọi thứ trừ chiếc bồn rửa bát trong nhà bếp – tất cả thư từ của chúng tôi về mọi chủ đề, mọi báo cáo được chuyển qua bàn làm việc của chúng tôi và hơn thế nữa.

Trong một số cách, đó là một lợi thế. Không có cơ hội đến một cuộc họp chỉ để phát hiện ra bạn đã bỏ quên tài liệu quan trọng nhất phía sau. Nhưng theo những cách khác, đó là một vấn đề lớn. Bằng cách mang theo quá nhiều thứ bên mình, bạn đang gặp nhiều rủi ro hơn.

Ví dụ, vào tháng 1 năm 2008, một chiếc máy tính xách tay đã bị đánh cắp từ xe của một sĩ quan tuyển dụng của Hải quân Hoàng gia. Nó chứa thông tin cá nhân về 600.000 người đã gia nhập lực lượng vũ trang của Anh, hoặc bày tỏ mong muốn làm như vậy[3] . Những vấn đề này có thể đã gây ra là rõ ràng. Như Bộ trưởng Bộ Quốc phòng vào thời điểm đó đã nói, không chỉ chi tiết về tài khoản ngân hàng bị tiết lộ mà cả địa chỉ nhà (và do đó là cuộc sống) của binh lính, thủy thủ và phi công.

Những sự cố như vậy là phổ biến. Cũng trong năm 2008, một cố vấn làm việc cho Bộ Nội vụ đã sao chép thông tin chi tiết của hàng nghìn tên tội phạm vào một thẻ nhớ – sau đó làm mất nó. Dữ liệu về 84.000 tội phạm đã bị đe dọa[4] . Vào năm 2009, một nhân viên hội đồng đã làm mất thẻ nhớ chứa tên và ngân hàng

[3] 'MoD bị mất ba máy tính xách tay không được mã hóa', ZDNet UK, ngày 22 tháng 1 năm 2008, http://news.zdnet.co.uk/security/0,1000000189,39292312,00.htm.

[4] 'Hãng "phá luật" vì mất dữ liệu', BBC News, 22 tháng 8 năm 2008, http://news.bbc.co.uk/1/hi/7575989.stm.

thông tin chi tiết của hơn 1.000 người nhận trợ cấp nhà ở[5] . Và vào năm 2010, nhà cung cấp dịch vụ chăm sóc sức khỏe của Mỹ, Kaiser Permanente, đã báo cáo rằng một thiết bị bị đánh cắp từ ô tô của một nhân viên có chứa hồ sơ liên quan đến 15.000 bệnh nhân[6] .

Chi phí ứng phó với những sự cố như vậy là rất lớn – Viện Ponemon cho biết các công ty Mỹ chi trung bình 204 đô la Mỹ cho mỗi hồ sơ khách hàng bị mất[7] .

Vậy chúng ta có thể làm gì để giảm khả năng xảy ra và hậu quả của sự cố?

Câu trả lời rõ ràng nhất là chỉ mang theo những gì bạn cần. Thật hấp dẫn khi mang thêm thông tin trên cơ sở 'chỉ trong trường hợp' hoặc vì việc tải xuống cơ sở dữ liệu hoàn chỉnh dễ dàng hơn là trích xuất các chi tiết cụ thể. Việc tạo một bản sao lưu trên thẻ nhớ USB có vẻ như là một biện pháp phòng ngừa hợp lý, nhưng điều đó cũng làm tăng gấp đôi khả năng dữ liệu của bạn sẽ bị thất lạc. Điều này cũng áp dụng cho các bản sao giấy và trong khi tài liệu giấy mang ít thông tin hơn PC, thông tin sẽ được hiển thị cho tất cả mọi người xem.

---

[5] 'Thanh dữ liệu hội đồng bị mất chứa chi tiết ngân hàng của 1.000 cư dân', dash.com, ngày 2 tháng 3 năm 2009, www.24dash.com/news/Local_Government/2009-03-02-Mất-hội-đồng-dữ-liệu-đính-chứa-chi-tiết-ngân-hàng-của-1-000-cư dân.

[6] 'Dữ liệu bệnh nhân của Kaiser bị đánh cắp', KRCA.com, ngày 12 tháng 1 2010, www.kcra.com/news/22220329/detail.html.

[7] 'Nghiên cứu Ponemon cho thấy chi phí vi phạm dữ liệu tiếp tục tăng', PR Newswire, ngày 25 tháng 1 năm 2010, www.prnewswire.com/news-releases/ponemon-study show-the-cost-of-a-data-breach- Continues -to-tăng 82585957.html.

Các phương tiện truy cập từ xa tốt hơn rất nhiều so với trước đây và dễ sử dụng hơn rất nhiều. Hơn nữa, các điểm truy cập công cộng đang lan rộng và Wi-Fi thậm chí còn có sẵn trên một số chuyến tàu. (Tuy nhiên, xin lưu ý rằng 'Wi-Fi công cộng miễn phí' không phải lúc nào cũng như vẻ ngoài của nó.)

Điều này loại bỏ nhu cầu mọi người mang theo quá nhiều dữ liệu bên mình. Nguyên tắc rất đơn giản: dữ liệu sẽ an toàn hơn rất nhiều khi nó được lưu giữ trên các máy chủ trung tâm được bảo mật và quản lý đúng cách. Vì vậy, lựa chọn tốt nhất là mọi người để nó ở đó và truy cập nó từ xa, khi cần thiết.

Nhưng còn dữ liệu mà mọi người thực sự phải mang theo thì sao? Vì vậy, mã hóa toàn bộ ổ đĩa cứng tích hợp và mã hóa ổ đĩa USB được thực thi tự động rất được khuyến khích. Nghe có vẻ phức tạp, nhưng không hề khó – hoặc tốn kém – để thực hiện. Các giải pháp dựa trên phần cứng có thể bảo mật toàn bộ đĩa theo các tiêu chuẩn vượt xa nhu cầu của hầu hết các tổ chức, hiện có sẵn với giá chỉ £200. Các giải pháp dựa trên phần mềm bảo vệ dữ liệu, từng tệp, vẫn rẻ hơn, ở mức £50 trở xuống cho một máy. Điều này nghe có vẻ nhiều, khi so sánh với việc giảm giá phần cứng máy tính. Chẳng hạn, bạn có thể mua một chiếc máy tính xách tay mạnh mẽ với giá vài trăm bảng Anh. Nhưng hãy nhớ rằng, dữ liệu trên thiết bị có thể có giá trị hơn nhiều so với chính thiết bị đó. Trong bối cảnh đó, mã hóa là một món hời.

Cũng nên nhớ rằng dữ liệu có giá trị đối với bạn cũng như đối với bất kỳ tên trộm nào. Nếu bản sao duy nhất của bạn trong số 300-báo cáo trang bạn vừa viết nằm trên chiếc máy tính xách tay vừa bị mất, nó thực sự có thể làm hỏng một ngày của bạn! Vì vậy, sao lưu công việc quan trọng của bạn,

lý tưởng là hàng ngày và giữ bản sao an toàn và cách xa bản gốc.

Cuối cùng, nó trả tiền để được cảnh giác. Không để các thiết bị và tài liệu có giá trị không được giám sát và ở nơi dễ thấy. Nếu bạn đang di chuyển bằng ô tô, hãy khóa máy tính xách tay của bạn trong cốp thay vì để nó ở chỗ có thể nhìn thấy. Hãy nhớ rằng ở một số quốc gia nước ngoài, hoạt động gián điệp công nghiệp rất phổ biến - và thậm chí còn được nhà nước bảo trợ - vì vậy các phòng khách sạn khóa kín không thể được coi là an toàn. Ngoài ra, hãy nhận biết những người xung quanh bạn trong khi bạn đang làm việc. Người đàn ông hoặc phụ nữ ngồi ở ghế sau có thể nhìn thấy thông tin nhạy cảm trên màn hình của bạn không? Và hãy cẩn thận với những gì bạn nói trên điện thoại ở những nơi công cộng. Hãy nghĩ xem hậu quả sẽ ra sao nếu ai đó làm việc cho một trong những đối thủ cạnh tranh khốc liệt nhất của bạn ngồi ở bàn bên cạnh.

Lời khuyên hàng đầu ...

Đừng mang theo nhiều dữ liệu hơn bạn phải mang theo.

Mã hóa đĩa và các thiết bị lưu trữ dữ liệu khác.

Tạo một bản sao lưu – mỗi ngày!

Đừng để thiết bị và tài liệu không được giám sát.

Cẩn thận với những con mắt tò mò.

'Tất cả các công việc tuyệt vời đang chuẩn
bị cho tai nạn xảy ra.'
Sidney Lumet

'Ối! ... Tôi đã làm điều đó một lần nữa.'
Britney Spears

Điều này đưa tôi đến chủ đề tiếp theo một cách thú vị – việc vô tình tiết lộ thông tin.

Ngay cả những người đứng đầu các tổ chức có ý thức bảo mật cũng vô tình tiết lộ dữ liệu mà họ đang cố gắng bảo vệ. Ví dụ, vào tháng 4 năm 2009, viên cảnh sát chống khủng bố cấp cao nhất của Anh bước ra khỏi ô tô và bước vào Phố Downing, tay ôm một chồng giấy tờ8 . Trên cùng của chồng, một trang được đánh dấu 'bí mật' được hiển thị rõ ràng. Nó đặt ra kế hoạch đập tan những gì được cho là một tế bào khủng bố ở Manchester.

Thật không may, những người ngoài cuộc bao gồm các nhiếp ảnh gia truyền thông, được trang bị máy ảnh độ phân giải cao, ống kính tele, v.v. Chính phủ đã hành động nhanh chóng để ngăn chặn những bức ảnh được công bố, nhưng sau đó con mèo đã ra khỏi túi. Để giảm thiểu 'thiệt hại', cuộc đột kích vào các cơ sở ở Manchester đã được tiến hành gấp rút. Người cảnh sát gây ra vấn đề

---

8 'Sai lầm khủng bố: Cảnh sát trưởng Bob Quick bị áp lực phải từ chức', The Daily Telegraph, 9 tháng 4 năm 2009, www.telegraph.co.uk/news/uknews/5128478/Terror-blunder-police-chief-Bob-Quick-under-pressure-to-resign.html.

đã từ chức ngay sau đó, nhưng ông không phải là người đầu tiên hoặc cuối cùng tiết lộ các tài liệu bí mật trong hoặc xung quanh Phố Downing.

Vào tháng 5 năm 2008, Caroline Flint, bộ trưởng nhà ở vào thời điểm đó, tiết lộ những lo ngại rằng giá nhà sẽ giảm 10% hoặc hơn trong năm đó và thị trường nhà mới đang sụp đổ9 .

Vào tháng 9 năm 2009, Lord Mandleson, khi đó là Bộ trưởng Kinh doanh, đã tiết lộ đánh giá về hoạt động của Đảng Lao động trong Chính phủ và các ý tưởng tấn công các đảng đối lập trong thời gian chuẩn bị cho cuộc bầu cử tiếp theo10.

Và đó mới chỉ là phần nổi của vấn đề. Mỗi ngày, có thể thấy hàng nghìn – có thể là hàng triệu – người đang có các cuộc trò chuyện bí mật và đọc các tài liệu bí mật trên tàu hỏa, trong phòng chờ sân bay và ở những nơi công cộng khác. Thật quá dễ dàng để vô tình bị lôi cuốn vào việc thảo luận những vấn đề bí mật với người lạ, hoặc với đồng nghiệp, trong bối cảnh xã hội, chỉ để khiến bản thân hoặc công việc của một người trở nên thú vị.

---

[9] 'Bộ trưởng sai lầm vạch trần những lo ngại bí mật của Chính phủ rằng giá nhà sẽ giảm ở mức tốt nhất là 5-10% trong năm nay', The Daily Mail, 13 tháng 5 năm 2008, www.dailymail.co.uk/news/article-566129/Bộ trưởng sai lầm-phơi bày- bí-quyết-Chính-phủ-sợ-giá-nhà-giảm-tốt-nhất-5-10-năm.html.

[10] 'Lord Mandelson là người mới nhất tiết lộ tài liệu bí mật ở Phố Downing', The Times, ngày 22 tháng 9 năm 2009, www.timesonline.co.uk/tol/news/politics/article6843506.ece.

2: Tình cờ tiết lộ

Như một Tweeter đã bình luận gần đây, 'Tôi không thể tin được cách mọi người đọc các tài liệu bí mật trên tàu cho cả thế giới xem. Tôi học được rất nhiều'.

Được cảnh báo!

Lời khuyên hàng đầu ...

Không đọc tài liệu mật ở nơi công cộng.

Không thảo luận những vấn đề bí mật ở nơi công cộng.

Nếu bạn phải mang các tài liệu bí mật ra khỏi văn phòng, hãy đặt chúng trong một phong bì, hoặc tốt hơn hết là một chiếc hộp có khóa.

CHƯƠNG 3: CON NGƯỜI LÀ THÔNG MINH

'Thông minh không phải là không phạm sai lầm, mà
là nhanh chóng biết cách sửa sai.'
Bertolt Brecht

Máy tính sẽ tuân theo các hướng dẫn một cách đáng tin cậy, miễn là chúng nhất quán và rõ ràng.
Con người có thể không làm theo những gì họ được bảo, nếu họ không nhìn thấy vấn đề, nhưng họ sẽ cố gắng hiểu những hướng dẫn không rõ ràng và có thể đối phó trong những tình huống mà hướng dẫn không được áp dụng.

Thông thường, nhân viên phải đối mặt với sự lựa chọn giữa việc tuân thủ, bằng cách tiếp tục công việc của họ, và gây ra sự chậm trễ và bất tiện, bằng cách tuân thủ chính sách bảo mật. Một ví dụ về điều này là chính sách yêu cầu nhân viên chỉ sử dụng tài khoản cá nhân của họ trong một môi trường như cửa hàng hoặc bệnh viện, nơi nhiều nhân viên dùng chung một thiết bị đầu cuối. Dưới áp lực về thời gian hoặc mong muốn trở nên hữu ích, sự cám dỗ là cho phép đồng nghiệp xử lý giao dịch trong phiên của bạn, thay vì đăng xuất và đăng nhập lại. Chỉ thực thi một chính sách, bằng các biện pháp kỹ thuật, hoặc bằng đe dọa trừng phạt, có thể phản tác dụng.

Nhân viên có thể trở nên mất động lực và bực bội nếu họ bị đối xử như một bánh răng trong máy hoặc một đứa trẻ ương ngạnh. Họ cũng có thể xác định biện pháp kiểm soát với chính sách, cảm thấy rằng nếu họ tìm ra cách vượt qua kiểm soát, họ sẽ không vi phạm chính sách. Hơn nữa, nếu một chính sách cụ thể được coi là không cần thiết, nhỏ nhặt, quan liêu, hoặc hoàn toàn sai lầm, thì toàn bộ vấn đề an ninh sẽ trở nên mất uy tín.

Tình hình có thể trở nên tồi tệ hơn bởi những khuyến khích năng suất ngây thơ. Nếu phần thưởng dựa trên số lượng công việc được xử lý, nhân viên sẽ tìm ra những cách khéo léo để tránh các biện pháp an ninh làm chậm chúng. Tệ hơn nữa, bảo mật sẽ bị coi là kẻ thù của công việc thực tế, thay vì là yếu tố đóng góp quan trọng cho sức khỏe của doanh nghiệp.

Phần mềm và công nghệ khác khó sử dụng và khó hiểu có thể gây ra các vấn đề tương tự. Ví dụ, nếu nhân viên sử dụng ý thức và phán đoán chung của họ để cân bằng giữa bảo mật và năng suất, thì họ cần phải có trong đầu một mô hình về cách thức hoạt động của công nghệ. Đây không phải là cấp độ kỹ thuật sâu, mà là cấp độ cho phép họ hiểu được hậu quả của những việc họ làm và các quyết định mà họ đưa ra.

Nếu công nghệ bảo mật đi kèm với một bộ hướng dẫn vận hành đơn giản là phải tuân theo, không cần biện minh hay giải thích, thì mọi người rất dễ bỏ lỡ một hoặc hai bước. Nếu mọi thứ dường như vẫn hoạt động và không có gì xấu xảy ra, họ sẽ đi đến một kết luận có vẻ như hiển nhiên - 'rõ ràng những bước đó không thực sự quan trọng'. Nhưng giả sử các bước còn thiếu là
liên quan đến việc mã hóa dữ liệu nhạy cảm trên đĩa CD để gửi qua đường bưu điện. Việc bỏ lỡ chúng sẽ không thành vấn đề nếu 99 trong số 100 lần phong bì được gửi đúng, nhưng trường hợp thứ 100 có thể dẫn đến các khoản tiền phạt đáng kể và tổn thất kinh doanh cho công ty, đồng thời có thể khiến nhân viên bị sa thải.

Điều tương tự cũng xảy ra đối với các quy trình kinh doanh và bảo mật. Các quy trình mà mọi người khó hiểu hoặc khó sử dụng sẽ dẫn đến sai sót và

'cải tiến' và loại bỏ các lỗ hổng trong bảo mật của họ. Ngược lại, các quy trình được thiết kế tốt và được giải thích rõ ràng sẽ cho phép nhân viên sử dụng ý thức chung và sự khéo léo của họ một cách xây dựng, khi họ gặp phải những trường hợp bất thường không được giải quyết trong hướng dẫn. Bạn không bao giờ biết, họ thậm chí có thể đưa ra một số cải tiến thực sự!

Không có giải pháp nhanh chóng và câu trả lời có thể áp dụng chung ở đây – quản lý, thúc đẩy và giáo dục mọi người là một công việc phức tạp. Thông điệp chính là bạn nên làm tất cả những gì có thể để 'đóng vòng lặp' và không ngừng phấn đấu để cải thiện. Tương tác với nhân viên của bạn, tìm hiểu ý kiến của họ và nếu có thể, hãy tính đến họ. Quan sát các hành vi thực tế và khi chúng đi chệch khỏi các thông lệ mong muốn, hãy cố gắng hiểu lý do tại sao và phản hồi các vấn đề đang bị đe dọa.

Chúng ta sẽ trở lại những vấn đề này sau.

Lời khuyên hàng đầu ...

Các quy trình bảo mật hoạt động tốt nhất khi chúng được tích hợp vào các ứng dụng và quy trình mà mọi người sử dụng, thay vì được thêm vào chúng.

Đảm bảo rằng mọi người hiểu lý do tại sao bạn yêu cầu họ làm mọi việc.

Kiểm tra các thủ tục của bạn phù hợp với cách mọi người thực sự làm việc.

Tìm kiếm và hành động dựa trên thông tin phản hồi.

Chính sách mật khẩu cung cấp một trường hợp nghiên cứu thú vị trong việc thiết kế các thủ tục bảo mật. Một số người nói rằng ngày của họ được đánh số - rằng sinh trắc học, thẻ thông minh và các công nghệ tương tự khác sẽ thay thế chúng - nhưng trong một thời gian đáng kể sắp tới, các tổ chức sẽ kiểm soát ai có thể truy cập mạng và hệ thống CNTT của họ, sử dụng tên người dùng và mật khẩu.

Để có hiệu quả về mặt bảo mật, chủ sở hữu mật khẩu phải được ghi nhớ, nhưng đối với tất cả ý định và mục đích, đó là một mớ ký tự ngẫu nhiên đối với bất kỳ ai khác.

Thật không may, mọi người thường chọn mật khẩu dễ nhớ – và gần như dễ đoán đối với người khác.

Vào tháng 1 năm 2010, một hacker vô danh đã đánh cắp danh sách 32 triệu mật khẩu từ RockYou, một công ty Mỹ phát triển phần mềm để sử dụng trên các trang mạng xã hội. Danh sách được đăng ngắn gọn trên một số trang web đã cung cấp một cái nhìn thú vị về mật khẩu mà người dùng thực sự chọn.

Theo một báo cáo trên tờ New York Times, cứ năm người dùng thì có một người để lại 'chìa khóa số tương đương với chìa khóa dưới thảm chùi chân', bằng cách chọn các mật khẩu dễ đoán, như 'abc123', 'iloveyou',

'qwerty' và thậm chí là 'mật khẩu'. Phổ biến nhất là '123456' 11.

Với mức độ dấu chân kỹ thuật số của hầu hết mọi người ngày nay, có thể nhiều mật khẩu ít phổ biến hơn sẽ dễ dàng bị tin tặc và kẻ lừa đảo tìm ra. Mọi người thường sử dụng những từ gắn liền với cuộc sống của họ làm mật khẩu – ví dụ như nơi sinh của họ, hoặc tên của trẻ em hoặc thú cưng – cho rằng những người lạ sẽ không biết những sự thật này. Vấn đề là những chi tiết như vậy ngày càng được đăng trên các trang mạng xã hội và ở các địa điểm công cộng khác. Mọi người cũng có xu hướng sử dụng cùng một mật khẩu cho mọi thứ, do đó, tính bảo mật kém trên một số trang web giải trí có thể dẫn đến việc tội phạm truy cập vào tài khoản ngân hàng hoặc e-mail công việc của bạn.

Các tổ chức coi trọng vấn đề bảo mật sẽ hạn chế các lựa chọn mà mọi người có thể đưa ra. Chúng yêu cầu mật khẩu bao gồm các chữ cái và chữ số, chữ hoa cũng như chữ thường, ký tự đặc biệt, chẳng hạn như %, < và * và vượt quá độ dài tối thiểu.

Hơn nữa, họ yêu cầu mật khẩu phải được thay đổi thường xuyên. Mặc dù tất cả những điều này khiến người khác khó đoán mật khẩu hơn, nhưng nó cũng khiến nó trở nên khó nhớ kinh khủng. Và tất nhiên, bạn không được viết nó ra!

Độ mạnh của mật khẩu là hàm của độ dài, độ phức tạp và tính ngẫu nhiên, trong số các tham số khác. Nó sẽ sử dụng đầy đủ bàn phím nhất có thể - không chỉ bao gồm

---

[11] 'Nếu mật khẩu của bạn là 123456, hãy đặt mật khẩu đó cho tôi', New York Times, ngày 20 tháng 1 năm 2010, www.nytimes.com/2010/01/21/technology/21password.html.

và chữ thường và số, nhưng dấu chấm câu và ký hiệu, nếu chúng được phép. Và nó sẽ càng dài càng tốt – tám ký tự thường được coi là mức tối thiểu.

Nhưng độ mạnh và bảo mật của mật khẩu không giống nhau. Độ mạnh làm cho mật khẩu khó đoán, nhưng thực tế có thể làm tăng khả năng bị tiết lộ, chẳng hạn như nếu nó buộc bạn phải ghi lại mật khẩu.

Việc viết ra danh sách mật khẩu có phải là một vấn đề hay không, tùy thuộc vào nơi danh sách được lưu giữ. Đồng nghiệp của tôi, Bruce Schneier, Giám đốc Công nghệ An ninh của BT, khuyến nghị rằng, nếu mọi người có ý định giữ một danh sách, họ nên sử dụng một mảnh giấy nhỏ và để nó ở nơi họ sẽ cất giữ những vật phẩm có giá trị tương tự – trong ví hoặc túi xách12. Bằng cách đó, họ sẽ biết ngay khi chúng bị mất hoặc bị đánh cắp và sẽ có thể thực hiện hành động tương ứng.

Một giải pháp thay thế an toàn hơn là sử dụng một tiện ích như Norton Identity Safe hoặc một tài liệu được mã hóa trên PC của bạn, để giữ chi tiết đăng nhập cho các ứng dụng và trang web riêng lẻ, đảm bảo rằng mật khẩu mở 'két sắt' điện tử của bạn là 'mạnh'.

Một chiến lược thay thế, do Sarah đề xuất Scalet, Biên tập viên cao cấp của Tạp chí CSO, trong Tháng 12 năm 2009, không phải để cố nhớ

---

[12] 'Viết lại mật khẩu của bạn', Schneier on Security, ngày 17 tháng 6 năm 2005, www.schneier.com/blog/archives/2005/06/write_down_y của chúng tôi.html.

mật khẩu cá nhân, nhưng để chọn một hệ thống tạo mật khẩu khó bẻ khóa13.

Cách tiếp cận mà cô ấy đề xuất – tương tự như cách tiếp cận do Microsoft và các tổ chức có ý thức bảo mật khác đề xuất – có 5 bước:

1 Chọn một số cụm từ bạn sẽ nhớ - có lẽ là những dòng đầu tiên của bài hát yêu thích. Ví dụ: dòng đầu tiên của Bài hát mật khẩu từ 'Tigger & Pooh and a Musical Too' là:
Kính vạn hoa hoặc trường mẫu giáo, Chú thỏ Phục sinh, Ông già Noel sẽ tặng 'kokebsc'.

2 Thay thế một số chữ thường bằng chữ in hoa, số hoặc ký hiệu, sử dụng các quy tắc bạn sẽ thấy dễ nhớ. Bạn có thể
bắt đầu và kết thúc bằng chữ in hoa, đồng thời thay thế các chữ cái 'o' và 'e' bằng '%' và '3'. Kết quả cuối cùng sẽ là 'K%k3bsC'.

3 Tùy chỉnh mật khẩu cho từng trang web hoặc ứng dụng bằng cách thêm ký tự hoặc số.
Để thực hiện việc này, hãy chọn một hệ thống lấy các ký tự từ tên của trang web hoặc chương trình mà bạn cần truy cập. Bạn có thể chọn hai ký tự đầu tiên của tên, tiếp theo là số lượng ký tự mà tên đó chứa. Điều đó sẽ tạo mật khẩu cho một tài khoản trên BT.com 'K%k3bsCBT6'.

4 Viết ra các gợi ý để nhắc bạn về các cụm từ và phương pháp bạn đã chọn. Giữ mảnh của

---

[13] 'Mật khẩu tốt là hệ thống tạo mã dễ nhớ nhưng khó bẻ khóa', Tạp chí CSO, ngày 15 tháng 12 năm 2009, http://
howto.techworld.com/security/3208751/how-to write-good-passwords .

giấy ở một nơi an toàn – có thể là trong ví hoặc túi xách của bạn.

5 Thay đổi mật khẩu của bạn định kỳ – nói, cứ sau 90 ngày. Hãy nhớ rằng – bạn không cần phải thay đổi mọi thứ. Bạn chỉ có thể thay đổi cụm từ là 'gốc' của mật khẩu của mình, giữ nguyên các quy tắc bạn sử dụng để thay thế các ký tự và liên kết mật khẩu với các trang web.

Hỗ trợ kỹ thuật cũng có sẵn dưới dạng nhiều ứng dụng quản lý mật khẩu.

Chúng có thể được sử dụng để tạo mật khẩu mạnh và lưu trữ chúng an toàn. Sau đó, bạn chỉ cần lo lắng về việc nhớ mật khẩu duy nhất cho phép bạn truy cập vào phần mềm quản lý mật khẩu.

CHƯƠNG 5: CON NGƯỜI LÀ GIÚP ĐỠ VÀ TIN TƯỞNG

'Bạn có thể bị lừa dối nếu quá tin tưởng, nhưng bạn sẽ sống trong dằn vặt nếu không đủ tin tưởng'. cần cẩu Frank

Nhân viên tin tưởng những người họ gặp trong quá trình làm việc là điều tự nhiên – đặc biệt là những người đang hoặc có vẻ là đồng nghiệp, khách hàng hoặc nhà cung cấp – và cố gắng hỗ trợ họ nếu họ cần giúp đỡ.

Chúng tôi được dạy từ đầu gối của mẹ rằng giữ cửa mở cho người đi sau là phép lịch sự.
Ngay cả khi chúng ta không thể nhìn thấy thẻ của họ, thì có lẽ nó nằm dưới chiếc áo khoác đó hoặc trong túi.

Nhưng doanh nhân ăn mặc bảnh bao đó đang vội vã lách qua cửa an ninh, rất có thể đang có ý định làm gián điệp công nghiệp. Còn nhóm mặc áo liền quần vừa đến mang theo dụng cụ và thang thì sao? Họ trông giống như các thành viên của đội bảo trì, nhưng đó có phải là con người thật của họ không? Không phải lúc nào bọn tội phạm cũng đeo mặt nạ, mặc áo có sọc và mang theo những chiếc túi được đánh dấu 'swag'!

Như một trang mạng xã hội ở Virginia, Michaele Salahi, và chồng của cô ấy, được thành lập vào tháng 11 năm 2009, bạn có thể tiếp cận tất cả các loại địa điểm nếu bạn quan sát kỹ phần này. Khi họ đến dự bữa tối cấp nhà nước tại Nhà Trắng, các nhân viên Sở Mật vụ tin chắc rằng họ là McCoy Thực sự, họ đã cho họ vào. Trong khi cặp đôi được sàng lọc bằng máy dò kim loại, v.v., 'các giao thức đã được thiết lập

đã không được theo dõi tại một điểm kiểm tra ban đầu'. (Dịch: không ai kiểm tra tên của Salahis trong danh sách khách mời.)14

Tương tự, điều quan trọng là mọi người phải nhớ rằng trộm cắp không phải là vấn đề duy nhất mà bạn đang bảo vệ cơ sở của mình chống lại. Ví dụ, vào năm 2005, những kẻ lừa đảo đã cố gắng đánh cắp khoảng 220 triệu bảng Anh từ Ngân hàng Sumitomo Mitsui bằng cách mang thiết bị vào văn phòng của ngân hàng này ở Thành phố Luân Đôn.
Mặc quần áo như nhân viên dọn vệ sinh, họ được một người trong cuộc – một nhân viên an ninh cho vào. Sau khi vào bên trong, họ kết nối các lỗi phần cứng với ổ cắm bàn phím của máy tính được sử dụng để thực hiện chuyển khoản ngân hàng. Và sau đó họ rời đi - không lấy gì cả.

Nhưng đó không phải là kết thúc của câu chuyện. Theo thời gian, các thiết bị này đã truyền các lần nhấn phím đến hang ổ của những kẻ lừa đảo gần đó. Dần dần, bọn tội phạm học được mọi thứ chúng cần để có thể chuyển một số tiền lớn vào tài khoản của chúng – mã người dùng, mật khẩu, chi tiết tài khoản khách hàng, v.v.
May mắn thay, các nhà chức trách đã nhận thức được những gì đang diễn ra và khi chuyển khoản ngân hàng được thực hiện, họ đã bị chặn15.

Ngay cả các chuyên gia bảo mật, người quản lý bộ phận trợ giúp CNTT, cũng khó cưỡng lại lời cầu xin của những cô gái điếm (và những người tương đương nam giới của họ) đang gặp nạn. Khi mọi người gọi để nói rằng họ đang làm việc

---

14 'Những kẻ phá cửa Nhà Trắng đã gặp Tổng thống Barack Obama', Bản tin BBC, 28 tháng 11 năm 2009, http://news.bbc.co.uk/1/hi/8383563.stm

15 'Bài học rút ra từ vụ trộm ngân hàng lớn nhất trong lịch sử', Cập nhật CIO, ngày 19 tháng 4 năm 2006, www.cioupdate.com/trends/article.php/3600126/Lessons-Học từ vụ cướp ngân hàng lớn nhất trong lịch sử.htm

đi vắng vài ngày, cần chuẩn bị vài thứ cho một cuộc họp quan trọng, nhưng lại quên mật khẩu, mật khẩu mới được cấp, nên người gọi có thể lấy bất cứ thứ gì họ cần.

Đây là một ví dụ về 'kỹ thuật xã hội', một cách được thiết lập tốt để khiến mọi người tiết lộ thông tin bí mật.

Khi thủ thuật lừa đảo lỗi thời này được tiến hành thông qua e-mail, nó được gọi là 'lừa đảo'. Theo nhà cung cấp bảo mật Internet, SonicWALL, 8,5 tỷ e-mail giả mạo đã được gửi đi mỗi tháng trong năm 200816.
Mỗi người đều tuyên bố là từ một tổ chức hợp pháp – chẳng hạn như ngân hàng – và bao gồm một yêu cầu rất giống nhau: yêu cầu người nhận xác minh tên người dùng, mật khẩu và các chi tiết khác của họ bằng cách truy cập một trang web.

Hầu hết mọi người bây giờ đều khôn ngoan đối với vấn đề này, điều này cũng tốt thôi - dòng email có rất ít dấu hiệu ngừng lại. Nhưng hàng năm, một tỷ lệ nhỏ – một báo cáo đưa ra con số là 12,5 trên mỗi triệu17 – làm sai những gì họ được yêu cầu. Họ truy cập trang web của kẻ lừa đảo, cung cấp thông tin chi tiết ... và thường phải trả giá.

Tội phạm mạng được cho là đã kiếm được 3,5 tỷ bảng Anh vào năm 2009 bằng cách lừa mọi người. Nghiên cứu của Văn phòng Thương mại Công bằng (OFT) của Anh cho thấy 73% người trưởng thành nhận được e-mail lừa đảo

---

[16] 'Bài kiểm tra IQ lừa đảo và spam SonicWALL', SonicWALL, www.sonicwall.com/phishing/.

[17] 'Có bao nhiêu người trở thành nạn nhân của các cuộc tấn công lừa đảo?', ZDNet, ngày 4 tháng 12 năm 2009, http://blogs.zdnet.com/security/?p=5084.

vào năm 2009, và kết quả là ba triệu người tiêu dùng Anh đã thiệt hại 3,5 tỷ bảng Anh18.

Các biến thể mới của kiểu tấn công này có thể cực kỳ tinh vi và khó phát hiện. Cái được gọi là 'spear phishing', được nhắm mục tiêu nhiều hơn so với lừa đảo qua email truyền thống và có thể nhắm vào nhân viên của một công ty cụ thể chẳng hạn.
Thêm vào e-mail những biệt ngữ của công ty, tên của các giám đốc điều hành và trưởng bộ phận, có thể làm cho nó có tính thuyết phục cao. Thậm chí chọn lọc hơn là 'lừa đảo cá voi' (vâng, tôi biết cá voi là động vật có vú, nhưng đó là tên gọi của nó), nhằm vào 'con cá lớn' cụ thể, chẳng hạn như CEO. Ví dụ về các cuộc tấn công săn bắt cá voi bao gồm trát hầu tòa giả mạo và thông báo thuế. Trong cơn hoảng loạn hoặc tức giận trước viễn cảnh bị kiện, nhà điều hành nhấp vào một liên kết được nhúng dẫn đến một trang web có giao diện thực tế. Những người bị nhắm mục tiêu có thể không bao giờ biết rằng do đó, phần mềm ghi nhật ký khóa đã được cài đặt trên PC của họ, để ghi lại mọi thứ họ nhập, bao gồm cả thông tin đăng nhập, cho phép truy cập vào thông tin thương mại nhạy cảm. (Nhân vật nữ chính được miêu tả trong Millennium Trilogy của Stieg Larsson sử dụng mánh khóe rất thành công19.)

Nó không chỉ là e-mail mà bạn phải xem.
Các cuộc tấn công cơ bản tương tự có thể sử dụng các kênh khác, chẳng hạn như tin nhắn nhanh và mạng xã hội.

---

18 'Chính phủ đàn áp lừa đảo trên mạng', Bộ cho Doanh nghiệp, Đổi mới và Kỹ năng, ngày 15 tháng 1 năm 2010, http://webarchive.nationalarchives.gov.uk/+/http://www.bis.gov.uk/news/features/2010/2/government-crackdown on-cyber-scams.

19 'Cô gái có hình xăm rồng' và các phần tiếp theo, Stieg Larsson, Quercus, 2008. Xuất bản lần đầu ở Thụy Điển, 2005.

5: Mọi người đều hữu ích và đáng tin cậy

Thật ngạc nhiên là mọi người sẽ làm gì để nhận được một món quà miễn phí. Trong vài năm, một thí nghiệm hàng năm được tiến hành bên ngoài ga Liverpool Street ở trung tâm London. Nhân viên văn phòng được tặng một thanh sô cô la nếu họ tham gia vào một cuộc khảo sát. Bảng câu hỏi yêu cầu họ cung cấp nhiều loại thông tin cá nhân khác nhau, bao gồm cả mật khẩu và tỷ lệ tuân thủ cao. Không ai thử kiểm tra mật khẩu, vì vậy có thể ít nhất một số đối tượng đã đánh lừa những người thử nghiệm bằng cách đưa ra mật khẩu sai. Tuy nhiên, có vẻ như một động cơ rất nhỏ, được đưa ra trong bối cảnh phù hợp, có thể đủ để khiến mọi người mù quáng trước những rủi ro đáng kể.

Một thí nghiệm khác liên quan đến việc phân tán thẻ nhớ USB xung quanh khuôn viên công ty, như thể chúng vô tình bị rơi. Chúng chứa một tải trọng phần mềm vô hại, chỉ gửi một tin nhắn lại cho những người thử nghiệm, khi họ được cắm vào PC. Tuy nhiên, chúng có thể đã mang theo phần mềm độc hại, có khả năng đánh sập mạng công ty, đánh cắp thông tin hoặc cung cấp quyền truy cập cửa sau để khai thác sau này. Một lần nữa, viễn cảnh về một thứ gì đó chẳng để làm gì khiến mọi người mất cảnh giác.

Để củng cố sự cần thiết phải cảnh giác với những người đam mê quà tặng, hãy xem xét trường hợp của nhân viên IBM, người đã vô tình phát tán các ổ USB bị nhiễm phần mềm độc hại tại hội nghị bảo mật AusCERT năm 2010. Công ty đã phải gửi một e-mail đáng xấu hổ cho tất cả những người tham dự hội nghị : 'Tại hội nghị AusCERT tuần này, bạn có thể đã nhận được một khóa USB miễn phí từ gian hàng của IBM... Thật không may, chúng tôi đã phát hiện ra rằng một số khóa USB này có chứa phần mềm độc hại và

chúng tôi nghi ngờ rằng tất cả các khóa USB có thể bị ảnh hưởng[20] . IBM không phải là công ty đầu tiên làm điều này, và chắc chắn sẽ không phải là công ty cuối cùng.

Lời khuyên hàng đầu ...

Không giả định gì cả – đảm bảo hoàn toàn chắc chắn rằng mọi người chính xác là người mà họ xuất hiện hoặc tuyên bố là.

Luôn cảnh giác với các nỗ lực kỹ thuật xã hội, thư rác và lừa đảo.

Không cắm bất cứ thứ gì vào PC nếu bạn không chắc nó đến từ đâu.

[20] 'IBM phát USB chứa đầy phần mềm độc hại', IT Pro, ngày 24 tháng 5 năm 2010, www.itpro.co.uk/623608/ibm-hands-out-malware-laden-usbs.

CHƯƠNG 6: KHAI THÁC CON NGƯỜI CÁC TÍNH CHẤT NÂNG CAO AN NINH

Như đã hứa, bây giờ tôi sẽ xem xét những gì có thể được thực hiện để tận dụng phẩm chất con người, nhằm cải thiện an ninh doanh nghiệp. Sau đó, chúng ta sẽ xem xét yếu tố con người trong mối quan hệ với quy trình và công nghệ.

Nhận thức và đào tạo là cơ bản. Mọi người chỉ có thể giúp ngăn chặn các hành vi vi phạm an ninh nếu họ nhận thức được các mối nguy hiểm và được hướng dẫn các hành vi an toàn như một phần trong quá trình đào tạo công việc thông thường của họ. Một doanh nghiệp phải thúc đẩy một nền văn hóa trong đó nhân viên chia sẻ trách nhiệm bảo vệ công ty khỏi bị tấn công – một nền văn hóa mà mọi người đều biết cách hành xử có trách nhiệm, cảnh giác với các vấn đề tiềm ẩn và hiểu những gì tốt nhất nên làm khi đối mặt với sự cố bảo mật tiềm ẩn.

Điều quan trọng là đào tạo bảo mật không chỉ giải thích những gì cần làm mà còn tại sao phải làm điều đó. Tất nhiên, thực tế là bảo mật hiệu quả là một yếu tố hỗ trợ kinh doanh và nâng cao thương hiệu của công ty – nó truyền cảm hứng cho niềm tin của khách hàng và đã được biết là giúp chốt nhiều thỏa thuận quan trọng. Vấn đề là điều này thường không được truyền đạt, dẫn đến kết quả là nhân viên chỉ nhận thức được 'cái gì' chứ không phải 'tại sao'.

Điều quan trọng nữa là mọi người phải hiểu được tác động to lớn mà các vi phạm an ninh có thể gây ra đối với danh tiếng và điểm mấu chốt của tổ chức.

Một chiến dịch nâng cao nhận thức đã được đánh giá cao là của Ngân hàng Barclays. trong số khác

vật liệu, công ty đã sản xuất một loạt video vừa thú vị vừa hiệu quả. Tại thời điểm viết bài, một số trong số này có thể được xem trên YouTube21. Hãy xem những điều này để biết làm thế nào một thông điệp nghiêm túc có thể được truyền tải theo cách thú vị và đáng nhớ, đồng thời khuyên nhân viên của bạn cũng nên làm như vậy.

Các nhóm cấp cao cần biết về trách nhiệm pháp lý cá nhân của họ theo luật pháp quốc tế và nhu cầu tuân thủ luật pháp như Đạo luật Sarbanes Oxley (SOX) của Hoa Kỳ, sau các vụ bê bối tài chính liên quan đến Enron, WorldCom và Arthur Andersen. Những người đứng đầu đôi khi coi bảo mật là chi phí chung và cần được thuyết phục rằng nó có thể nâng cao Lợi tức đầu tư (ROI) và thúc đẩy lợi nhuận của doanh nghiệp. Các nhà quản lý cấp trung, đặc biệt là những người trong bộ phận bán hàng và tiếp thị, cần biết rằng một chính sách bảo mật hiệu quả có thể giúp chốt được các giao dịch, như một cách trực tiếp để nâng cao niềm tin của khách hàng. Lực lượng lao động nói chung nên nhận thức được rủi ro và được khuyến khích 'đóng cửa', cả về vật chất và điện tử. Điều này bao gồm mọi thứ từ việc bảo vệ máy tính xách tay và BlackBerry của họ, cho đến việc đảm bảo rằng mật khẩu được thay đổi thường xuyên và báo thức được đặt bởi người cuối cùng rời khỏi tòa nhà. Đào tạo dựa trên máy tính là một cách hiệu quả về chi phí để giữ cho nhận thức và kỹ năng của mọi người được cập nhật.

Ngoài điều này, điều quan trọng là mọi người phải tham gia bảo vệ tổ chức,

[21] Video nâng cao nhận thức về bảo mật của Ngân hàng Barclays: www.youtube.com/user/JonathanRhodesDotCom.

bắt đầu lại từ đầu. Một chiến dịch nâng cao nhận thức và đào tạo sẽ bị hủy hoại nếu các giám đốc điều hành, quản lý cấp cao và cấp trung không hoàn toàn ủng hộ nó. Điều này cần vượt ra ngoài những mỹ từ và cách nói; các nhà lãnh đạo phải được coi là áp dụng các hành vi an toàn mà họ khuyến khích người khác làm theo.

Trích dẫn Khảo sát năm 2008 của Bộ Kinh doanh, Doanh nghiệp và Cải cách Quy định22 của Vương quốc Anh, Vi ninh Thông tin 'Ví dụ về các hành vi phạm An tích cực thể hiện mức độ ưu tiên cao bao gồm hiểu biết về CNTT ở cấp hội đồng quản trị, nhấn mạnh vào các quy trình kiểm soát truy cập và sao lưu hiệu quả, sẵn sàng chi tiền và tham gia thường xuyên vào các vấn đề bảo mật. Các hành vi thể hiện mức độ ưu tiên thấp bao gồm muốn được bảo vệ mà không sẵn sàng trả tiền cho việc đó, thiếu hành động sau khi vi phạm an ninh, kém hiểu biết về các vấn đề kỹ thuật và quá ít chú ý đến việc nâng cao nhận thức của nhân viên'.

Cách các nhà quản lý phản ứng với các vi phạm là đặc biệt quan trọng. Số liệu thống kê cho thấy khoảng 80% tội phạm điện tử là do những người không có ý định làm điều gì sai trái, nhưng vô tình gây ra hoặc kích hoạt, gây ra hoặc kích hoạt23.

---

[22] 'Khảo sát vi phạm an ninh thông tin năm 2008', Cục Cải cách Doanh nghiệp, Doanh nghiệp và Quy định, tháng 4 năm 2008, www.security-survey.gov.uk.

[23] 'Infosec: không còn chỉ là mối quan tâm của bộ phận CNTT', Tạp chí SC, tháng 5 năm 2005, www.scmagazineus.com/infosec-no-longer-just-the-it department-concern/article/32152/.

6: Khai thác phẩm chất con người để cải thiện Bảo vệ

Bài học ở đây rất đơn giản – nếu bạn muốn giữ mọi người đứng về phía mình, thì điều cần thiết là không được 'kết tội' bất kỳ ai chỉ đơn giản là phạm sai lầm.
Có một mối nguy hiểm là các vấn đề có thể bị giấu nhẹm – cứ để đó âm ỉ cho đến khi chúng thực sự trở nên rất nghiêm trọng. Thay vào đó, điều cần thiết là một môi trường cởi mở và hỗ trợ, khuyến khích mọi người 'làm quen'. Bằng cách đó, tổ chức có cơ hội học hỏi từ những sai lầm của mình – đóng cửa chuồng ngựa trước khi những con ngựa có giá trị có cơ hội chạy trốn hoặc bị đánh cắp. Khả năng mọi người sẽ báo cáo các vấn đề, sẽ phụ thuộc vào sự tin tưởng của họ đối với hệ thống báo cáo, có thể được điều hành bởi chủ lao động của họ, một cơ quan độc lập hoặc cơ quan chính phủ. Họ sẽ không chỉ lo lắng về việc bản thân có thể bị trừng phạt và truy tố mà còn lo lắng về việc bảo vệ danh tính của mình nếu họ báo cáo những sai sót và vi phạm của người khác. Ngành hàng không đã sử dụng thành công các chương trình báo cáo, khuyến khích người lao động báo cáo các sự cố liên quan đến an toàn.

Lời khuyên hàng đầu ...

Huấn luyện mọi người về an ninh.

Giải thích cả 'cái gì' và 'tại sao'.

Chạy các khóa bồi dưỡng thường xuyên.

Bảo mật bắt đầu từ cấp cao nhất, với Giám đốc điều hành. Người đó phải làm gương sáng.

Tạo điều kiện dễ dàng – và an toàn – để mọi người báo cáo lỗi... ngay cả khi đó là lỗi của Giám đốc điều hành!

CHƯƠNG 7: TẠI SAO PHẢI NÂNG CAO NHẬN THỨC?

Theo Mạng lưới châu Âu và
Cơ quan An ninh Thông tin (ENISA)24, một chương trình nâng cao nhận thức về an ninh thông tin sẽ:

Cung cấp đầu mối và động lực cho một loạt các hoạt động nâng cao nhận thức, đào tạo và giáo dục liên quan đến an toàn thông tin, một số hoạt động có thể đã được thực hiện, nhưng có lẽ cần được phối hợp tốt hơn và hiệu quả hơn.

Truyền đạt các nguyên tắc hoặc thực tiễn được đề xuất quan trọng, cần thiết để bảo mật các nguồn thông tin.

Cung cấp thông tin chung và cụ thể về các biện pháp kiểm soát và rủi ro bảo mật thông tin cho những người cần biết.
Làm cho các cá nhân nhận thức được trách nhiệm của họ liên quan đến bảo mật thông tin.

Khuyến khích các cá nhân áp dụng các hướng dẫn hoặc thực hành được khuyến nghị.
Tạo ra một nền văn hóa bảo mật mạnh mẽ hơn, một nền văn hóa có hiểu biết rộng và cam kết bảo mật thông tin.

Giúp tăng cường tính nhất quán và hiệu quả của bảo mật thông tin hiện có

---

24 Hướng dẫn 'Người dùng mới': Cách khai thác thông tin nhận thức về bảo mật', ENISA, ngày 1 tháng 7 năm 2008, www.enisa.europa.eu/act/ar/deliverables/2008/new_users-guide/?searchterm=information_security chương trình.

và có khả năng kích thích việc áp dụng các biện pháp kiểm soát hiệu quả về chi phí.

Giúp giảm thiểu số lượng và mức độ vi phạm an ninh thông tin, do đó giảm chi phí trực tiếp (ví dụ: dữ liệu bị vi-rút làm hỏng) và gián tiếp (ví dụ: giảm nhu cầu điều tra và giải quyết các vi phạm); đây là những lợi ích tài chính chính của chương trình.

bài tập tình huống BT

BT đã phát triển một loạt các chương trình nhằm phòng ngừa, giáo dục và đào tạo nâng cao nhận thức.

Mọi người trong công ty được yêu cầu hoàn thành gói Đào tạo dựa trên máy tính (CBT) hai năm một lần và có các phòng khám an ninh trong toàn công ty cũng như các buổi giới thiệu trên toàn cầu để nâng cao nhận thức. Công ty thậm chí đã giới thiệu một kế hoạch trao phần thưởng tài chính cho những người thể hiện hành vi bảo mật tốt.

BT cũng cung cấp bộ phận trợ giúp 24/7 để cung cấp trợ giúp và lời khuyên cho nhân viên của mình. Bộ phận trợ giúp nhận 20.000 cuộc gọi mỗi năm từ những người báo cáo sự cố và công ty hy vọng sẽ thu thập thêm các báo cáo thông qua mạng nội bộ của mình.

Điều quan trọng nữa là đảm bảo rằng các quy trình kinh doanh của tổ chức được thiết kế để thực thi lại các chính sách bảo mật của tổ chức. Ví dụ: trong khi Cảnh sát Thành phố Luân Đôn tin rằng chỉ có 25% tội phạm được báo cáo, các quy trình của BT buộc người của họ phải làm như vậy. Cho dù đó là một chiếc ô tô bị hư hỏng hay một chiếc máy tính xách tay bị đánh cắp, không một món đồ nào được thay thế hoặc sửa chữa nếu không có Số Tham chiếu Tội phạm, điều này sẽ kích hoạt hệ thống thích hợp.

7: Tại sao phải nâng cao nhận thức?

Gần đây, công ty đã phân phát một cuốn sách nhỏ có tựa đề 'BT Security: Your Part in the Big Picture', cho tất cả nhân viên. Điều này mô tả 18 hành vi bảo mật mong muốn. Định dạng bỏ túi khuyến khích nhân viên mang theo bên mình trong áo khoác hoặc túi đựng máy tính xách tay.

CHƯƠNG 8: NGOẠI CẢNH

Các chiến dịch nâng cao nhận thức và đào tạo bắt buộc cũng quan trọng như vậy, nhưng chúng chỉ có thể tiến xa.
Đào tạo hoạt động tốt nhất khi nó thường xuyên được củng cố bằng kinh nghiệm và đây là một vấn đề trong trường hợp bảo mật. Bảo mật thành công được đánh giá bằng sự vắng mặt của các sự kiện xấu hơn là sự xuất hiện của những sự kiện tốt. Do đó, các cơ hội để củng cố hành vi tích cực bị hạn chế. Như đã đề cập ở trên, trừng phạt nhân viên liên quan đến vi phạm an ninh, ngoại trừ các trường hợp cố ý hoặc liều lĩnh trắng trợn, không phải là một ý tưởng hay. Nó khuyến khích sự bí mật, và cản trở việc học hỏi, ở cấp độ cá nhân và tổ chức.

Vì những lý do tương tự, việc đo lường hiệu quả của các chiến dịch nâng cao nhận thức và đào tạo có thể khó khăn. Nhưng nó cần phải được thực hiện. Sẽ rất dễ dàng để chi tiền cho các áp phích, trang web và đào tạo dựa trên máy tính, rồi tự mãn ngồi lại và nghĩ rằng 'công việc đã hoàn thành'. Tốt hơn hết là tiếp cận vấn đề một cách khoa học. Đầu tiên, hãy tìm ra những gì bạn đang thực sự cố gắng cải thiện. Bạn đang cố gắng giảm trộm cắp? Hay rò rỉ thông tin? Hay lừa đảo?
Điều này sẽ giúp tập trung chiến dịch của bạn, ngoài bất kỳ điều gì khác. Sau đó tìm cách định lượng vấn đề. Thiết lập một số liệu cơ bản và theo dõi xem điều này thay đổi như thế nào khi chiến dịch tiến triển.
Tiếp tục đo nó sau đó, vì lợi ích có thể giảm dần khi ký ức mờ dần. Bằng cách sử dụng một loạt các thước đo thành công khác nhau, bạn sẽ tránh được việc tập trung quá hẹp. Bạn có thể muốn xem lại các biện pháp của mình theo định kỳ, vì các ưu tiên và bản chất của các mối đe dọa mà doanh nghiệp của bạn phải đối mặt sẽ thay đổi.

8: Ngoài Nhận Thức

Với điều kiện là thông tin không quá nhạy cảm, việc xuất bản các chỉ số bảo mật trong tổ chức của bạn có thể giúp thu hút sự tham gia của nhân viên. Nó hỗ trợ động lực nếu mọi người có thể cảm thấy những nỗ lực của họ đang có một số hiệu quả.

Mục đích cuối cùng là để nhân viên của bạn tham gia đầy đủ vào một chương trình cải tiến liên tục nhằm tối ưu hóa hiệu suất của doanh nghiệp về mặt bảo mật thông tin. Đây là một chương trình khả thi về các mức thành tích, được trình bày theo cách thức của một mô hình trưởng thành năng lực:

Đặc biệt: Không có chương trình nâng cao nhận thức hoặc đào tạo có tổ chức. Quy trình và thủ tục là chắp vá, tốt nhất.

Nhận thức: Tổ chức chiến dịch để làm cho tất cả nhân viên nhận thức được các vấn đề bảo mật, các mối đe dọa và cạm bẫy. Chính sách bảo mật được ghi lại và có sẵn cho tất cả nhân viên.

Được đào tạo: Các quy trình bảo mật dành riêng cho công việc được thiết lập và ghi lại, đồng thời được giảng dạy như một phần không thể thiếu của đào tạo, cho các vai trò cá nhân và nhóm.

Được đào tạo: Nhân viên hiểu biết về các mối đe dọa và biện pháp kiểm soát bảo mật cũng như các kỹ thuật quản lý rủi ro, cho phép họ đưa ra các quyết định thông minh, sáng suốt trong công việc hàng ngày và khi phát sinh các trường hợp ngoại lệ.

Được trao quyền: Mọi người trong toàn doanh nghiệp có thể và đáng tin cậy để đóng góp cá nhân vào việc cải tiến liên tục bảo mật doanh nghiệp. Điều này có thể hoạt động theo cách tương tự như các chương trình Quản lý Chất lượng Toàn diện lấy cảm hứng từ bài viết của

8: Ngoài Nhận Thức

William Edwards Deming, người đã giúp chuyển đổi ngành công nghiệp Nhật Bản vào nửa sau của Thế kỷ 20.

Lời khuyên hàng đầu ...

Đo lường hiệu quả của các chiến dịch nâng cao nhận thức và đào tạo.

Thu hút nhân viên, để thúc đẩy cải tiến liên tục.

CHƯƠNG 9: SỰ MỞ RỘNG DOANH NGHIỆP

'Công ty {lớn} trung bình có thông tin nhạy cảm trị giá 12 triệu đô la Mỹ ở nước ngoài.'
McAfee, 200925

Trong thế giới phức tạp và đầy thách thức ngày nay, rất ít công ty có thể tự làm mọi thứ. Hầu hết cần tập trung vào lĩnh vực mà họ xuất sắc và nhờ đến chuyên môn bên ngoài để hoàn thành các nhiệm vụ khác. Nếu nhà thầu gia công phần mềm cần quyền truy cập vào dữ liệu cá nhân hoặc nhạy cảm, bạn cần xem xét nhận thức về bảo mật của nhân viên của họ, cũng như của chính bạn. Do đó, điều quan trọng là phải đánh giá các chính sách, quy trình và văn hóa bảo mật của nhà thầu, như một phần không thể thiếu trong quy trình lựa chọn.

Chính sách bảo mật mẫu về gia công phần mềm do Diễn đàn những người triển khai ISO27k soạn thảo, làm rõ những gì các công ty nên mong đợi26:

5.4.3 Nhận thức, đào tạo và giáo dục về bảo mật thông tin phù hợp sẽ được cung cấp cho tất cả nhân viên và bên thứ ba làm việc trong hợp đồng, làm rõ trách nhiệm của họ liên quan đến bảo mật thông tin của <TỔ CHỨC>

---

[25] 'Nền kinh tế không an toàn, bảo vệ thông tin quan trọng', McAfee, 2009, http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

[26] 'Chính sách bảo mật thông tin về thuê ngoài, Diễn đàn những người triển khai ISO27k, 2008, www.iso27001security.com/ISO27k_model_policy_on_outhuê_ngoài.doc.

chính sách, tiêu chuẩn, quy trình và hướng dẫn (ví dụ: chính sách quyền riêng tư, chính sách sử dụng được chấp nhận, quy trình báo cáo sự cố bảo mật thông tin, v.v.) và tất cả các nghĩa vụ liên quan được xác định trong hợp đồng.

Gia công phần mềm không có gì mới, tất nhiên. Mọi người đã làm điều đó trong nhiều thế kỷ. Điều khác biệt bây giờ là thế giới đã trở thành kỹ thuật số và dữ liệu máy tính có thể được chuyển dễ dàng đến các tổ chức ở phía bên kia hành tinh, cũng như bất kỳ nơi nào khác. Và nếu các tổ chức ở các quốc gia khác nhau, các yếu tố như sự khác biệt về ngôn ngữ và văn hóa, sẽ gây ra những mối nguy hiểm bổ sung.

Điều này đặt ra một số câu hỏi thú vị. Khi thế giới của chúng ta ngày càng kết nối với nhau, nó có trở nên rủi ro hơn không? Giả sử bạn thuê một nhà cung cấp dịch vụ thuê ngoài việc quản lý bảng lương của mình. Rủi ro mà bạn phải đối mặt tăng lên hay giảm xuống? Nhà cung cấp có trụ sở ở đâu hay công việc có quan trọng không? Hoặc nhân viên của họ thực sự có ý thức bảo mật như thế nào?

Cũng như nguy cơ tiết lộ thông tin thực tế, có khả năng bạn đang vi phạm pháp luật chỉ bằng cách gửi dữ liệu đến một quốc gia khác. Luật pháp châu Âu cấm xuất khẩu dữ liệu cá nhân sang các quốc gia không đáp ứng tiêu chuẩn 'đầy đủ' của châu Âu về bảo vệ quyền riêng tư. Thật thú vị, Hoa Kỳ không đủ điều kiện, do cách tiếp cận pháp lý khác nhau đối với quyền riêng tư. Điều này dẫn đến việc đàm phán về khuôn khổ 'bến cảng an toàn', đơn giản hóa quy trình mà theo đó các công ty Hoa Kỳ có thể được chấp thuận nhận dữ liệu từ châu Âu, trên cơ sở kiểm soát nội bộ của họ.

Tình hình đã tốt hơn so với vài năm trước, khi các phương tiện truyền thông tràn ngập những câu chuyện về nhân viên tổng đài sẵn sàng bán chi tiết tài khoản ngân hàng của khách hàng và các dữ liệu bí mật khác cho bọn tội phạm.

Luật bảo vệ dữ liệu đã được thắt chặt, nhưng ngay cả ngày nay, các tiêu chuẩn mà các công ty ở một số quốc gia áp dụng vẫn chưa đạt được mức có thể chấp nhận được ở Anh, Châu Âu hoặc Hoa Kỳ.

Vào tháng 4 năm 2009, Cơ quan Dịch vụ Tài chính của Anh - cơ quan quản lý các ngân hàng, công ty bảo hiểm, v.v. - cho biết việc đào tạo nhân viên tại các trung tâm cuộc gọi ở nước ngoài "nhìn chung là kém" và kêu gọi các công ty làm nhiều hơn để đảm bảo rằng nhân viên làm việc thay mặt họ. được trang bị phù hợp để phát hiện và báo cáo các vấn đề bảo mật27.

Lời khuyên hàng đầu ...

Đánh giá các chính sách, quy trình và văn hóa bảo mật của nhà thầu, như một phần không thể thiếu trong quy trình lựa chọn.

Nếu các nhà thầu ở nước ngoài, hãy đảm bảo rằng bạn có quyền gửi dữ liệu khách hàng cho họ trước khi thực hiện.

27 'Nhân viên kém kiểm tra tại các trung tâm cuộc gọi ở nước ngoài gây ra rủi ro tội phạm', Cố vấn FT, ngày 28 tháng 4 năm 2009, www.ftadviser.com/FTAdviser/Regulation/Regulators/FSA/Tin_tức/bài_viết/20090428/b813beec-33d9-11de-baf8-00144f2af8e8/Poor-staff-vetting-at-offshore-call-centres-pose-crime-risks.jsp.

'Thiết kế ra khả năng xảy ra lỗi của con người dẫn đến vi phạm an ninh mạng, là cách tiếp cận tối ưu để giải quyết vấn đề. Nếu không có khả năng xảy ra lỗi do con người (hãy nghĩ đến việc nâng cấp phần mềm bảo mật tự động thay vì do người dùng cài đặt), thì điều đó sẽ không xảy ra.'
Mạng chuyển giao kiến thức an ninh mạng28

Bảo mật về cơ bản là quản lý các loại rủi ro hoạt động nhất định, thường được gọi là 'CIA' – Bảo mật, Toàn vẹn và Sẵn có.

Các tiêu chuẩn, chẳng hạn như ISO27001, cung cấp hướng dẫn thực hành tốt nhất trong việc thiết kế, thiết lập, vận hành và cải thiện các thể chế và thủ tục, dựa trên các nguyên tắc quản lý rủi ro. Chúng được gọi là Hệ thống quản lý bảo mật thông tin.

Tuy nhiên, điều quan trọng là phải tính đến bảo mật khi thiết kế các quy trình kinh doanh thông thường. Bảo mật có xu hướng là 'Cô bé lọ lem' yêu cầu, được coi là một phần bổ sung muộn, hoặc hồi tố, do vi phạm hoặc suýt bỏ lỡ. Kết quả là, xung đột giữa bảo mật và, chẳng hạn như năng suất, không được công nhận chứ chưa nói đến việc giải quyết thỏa đáng.

---

28 'Sai lầm là con người, để thiết kế ra thần thánh', An ninh mạng Mạng chuyển giao tri thức, 2007, http://server.quid5.net/~koumpis/pubs/pdf/cybersecurity2007.pdf.

10: Thiết kế quy trình

Các chuyên gia về yếu tố con người sẽ phân loại các quy trình bảo mật là "nhiệm vụ hỗ trợ" chứ không phải là "nhiệm vụ sản xuất". Các nhiệm vụ sản xuất liên quan đến hoạt động tạo ra giá trị cơ bản hàng ngày và bất kỳ điều gì cản trở chúng đều được chú ý ngay lập tức và được giải quyết như một ưu tiên cao.
Các nhiệm vụ hỗ trợ thường có lợi ích lâu dài và trong ngắn hạn, có thể được coi là "cản đường". Do đó, các thủ tục an ninh làm mất thời gian của công việc bình thường, đòi hỏi nỗ lực thể chất hoặc sự tập trung tinh thần, sẽ bị bỏ qua. Để chống lại xu hướng này, bảo mật phải được tích hợp vào các nhiệm vụ và quy trình kinh doanh của mọi người, thay vì can thiệp vào chúng.

Chuyển giao kiến thức an ninh mạng Vương quốc Anh
Mạng cung cấp các nguyên tắc hữu ích sau29:

Xác định các yêu cầu thực hiện của nhiệm vụ sản xuất và đảm bảo rằng nhiệm vụ bảo mật không làm giảm đáng kể năng suất.

Giảm thiểu khối lượng công việc về thể chất và tinh thần của nhiệm vụ bảo mật; sử dụng một phương thức tương tác phù hợp với hoạt động của nhiệm vụ sản xuất (ví dụ: cơ chế dựa trên giọng nói, tương tác dựa trên điện thoại hoặc cơ chế rảnh tay, để

[29] 'Lỗ hổng con người trong các hệ thống an ninh', An ninh mạng Nhóm làm việc về nhân tố con người KTN, 2007, http://hornbeam.cs.ucl.ac.uk/hcs/publications/HFWG%20Trắng%20Paper%20Final.pdf.

nhiệm vụ mà cả hai tay đều bận rộn).

Đối với các cơ chế bảo mật được thực thi thường xuyên, hãy thiết kế cho tốc độ; ít sử dụng cơ chế, thiết kế để ghi nhớ (hướng dẫn người dùng từng bước, giao diện dựa trên nhận dạng).

Giảm thiểu phạm vi cho lỗi. Nghiên cứu về yếu tố con người, đặc biệt là nghiên cứu về lỗi của con người, cung cấp nhiều hướng dẫn về cách thiết kế các hệ thống nhằm giảm thiểu khả năng xảy ra lỗi và tác động của lỗi. Các hệ thống phải được thiết kế sao cho một lỗi đơn lẻ của một cá nhân không dẫn đến các sự cố bảo mật nghiêm trọng.

Khuyến khích hành vi an toàn (cũng như – hoặc là một khía cạnh của – mục tiêu năng suất).

CHƯƠNG 11: KHẢ NĂNG SỬ DỤNG

'Một sự cân bằng tốt hơn phải được tìm thấy giữa những hạn chế của con người và mong muốn tăng cường an ninh. Cần nghiên cứu thêm về mối quan hệ giữa nhận thức về khả năng sử dụng, bảo mật và sự tiện lợi.'

Hoonakker và cộng sự30

'Tại sao máy tính của bạn làm phiền bạn rất nhiều về bảo mật, nhưng vẫn không an toàn? Đó là vì người dùng không có mô hình bảo mật hoặc cách đơn giản để giữ an toàn cho những thứ quan trọng.'

Quản gia Lampson31

Butler Lampson32 trích dẫn hai lý do chính khiến phần mềm không an toàn: lỗi và xung đột. Những xung đột mà anh ấy đang đề cập đến là giữa mong muốn có nhiều chuông và còi hơn, thời gian đưa sản phẩm ra thị trường nhanh hơn, chi phí thấp hơn và tính bảo mật cao hơn. Đối với những điều này, tôi sẽ thêm khả năng sử dụng kém như một vấn đề khác biệt.

---

30 'Xác thực mật khẩu từ góc độ yếu tố con người: kết quả khảo sát giữa những người dùng cuối', Hoonakker, Bornoe và Carayon, Kỷ yếu Hội nghị thường niên lần thứ 53 của Hiệp hội Nhân tố Con người và Công thái học, tháng 10 năm 2009, www.hfes.org/web/Newsroom /HFES09-Hoonaker CIS.pdf.

31 'Usable security: how to get it', Butler Lampson, Communications of the ACM, tập 52, số 11, tháng 11 năm 2009, trang 25.

32 'Usable security: how to get it', Butler Lampson, Communications of the ACM, tập 52, số 11, tháng 11 năm 2009, trang 25.

Bất kể bạn dành bao nhiêu tiền để cố gắng giáo dục mọi người về bảo mật thông tin, bạn sẽ phải đối mặt với một cuộc đấu tranh khó khăn nếu hệ thống và quy trình của bạn khó hiểu hoặc khó sử dụng đối với họ. Có hai cách nhìn nhận vấn đề, được coi là cách tiếp cận bổ sung tốt nhất, được sử dụng kết hợp:

- Đừng tạo cơ hội cho người dùng làm những điều xấu hoặc ngu ngốc: Nếu một chính sách là bắt buộc, hãy thực thi chính sách đó thông qua tự động hóa, nếu có thể. Nếu các quyết định quá phức tạp đối với người dùng bình thường, thì có thể tốt hơn là thực thi một lựa chọn an toàn (mặc dù dưới mức tối ưu). Cân nhắc việc tạo các lớp người dùng, dựa trên mức độ chuyên môn, với nhiều quyền quyết định hơn dành cho người dùng chuyên gia.
- Giúp người dùng đưa ra lựa chọn tốt: Khi người dùng cần đánh giá hoặc đưa ra quyết định, hoặc mong muốn, hãy làm cho việc đưa ra quyết định đúng đắn dễ dàng nhất có thể. Cung cấp một mô hình nguyên nhân và kết quả trực quan mà người dùng có thể liên quan đến. Trình bày thông tin cần thiết để đưa ra quyết định một cách rõ ràng. Giải thích ý nghĩa của các lựa chọn khác nhau. Áp dụng các nguyên tắc thiết kế giao diện người dùng tốt để giảm thiểu khả năng mắc lỗi.

Việc tìm kiếm các nguyên tắc thiết kế chi phối sự tương tác của con người với công nghệ, là một lĩnh vực nghiên cứu ứng dụng và học thuật trưởng thành, được gọi là các yếu tố con người, tương tác giữa con người và máy tính, thiết kế giao diện người-máy, khả năng sử dụng, v.v., tùy thuộc vào trọng tâm.

Một số công ty thậm chí còn có phòng thí nghiệm chuyên môn để kiểm tra khả năng sử dụng. Nói chung, nó là một thứ nghệ thuật đen, hơn là khoa học kỹ thuật, mặc dù trong một số

các lĩnh vực, các nguyên tắc được thiết lập tốt vẫn tồn tại. Ví dụ bao gồm các điều khiển trong ô tô, thiết kế buồng lái máy bay và giao diện WIMP (cửa sổ, biểu tượng, menu, con trỏ) quen thuộc hiện nay trên máy tính. Tất cả đều là kết quả của nhiều năm cùng tiến hóa, theo đó các nhà thiết kế đã đáp ứng trải nghiệm của người dùng và người dùng đã học được các mô hình tinh thần cho phép họ sử dụng các điều khiển

một cách trực giác. Kết quả là người lái xe có thể thích nghi với một chiếc ô tô mới chỉ trong vài giây và chủ sở hữu Macintosh có thể nắm bắt những kiến thức cơ bản về giao diện Windows® mà không cần hướng dẫn.

Thật không may, chúng tôi hiểu tương đối ít về chính xác cách mọi thứ được thiết kế làm tăng – hoặc giảm – khả năng người dùng sẽ vô tình làm những việc khiến các tổ chức bị tấn công.

Một nghiên cứu được thực hiện bởi các nhà nghiên cứu tại Đại học Wisconsin-Madison và Đại học CNTT Copenhagen đã làm sáng tỏ tình hình33.
Tập trung vào cách người dùng chọn mật khẩu, nó phát hiện ra rằng các chuyên gia bảo mật cũng có khả năng đi chệch khỏi thực tiễn tốt nhất giống như người dùng phổ thông. Điều quan trọng nhất là kinh nghiệm, không phải chuyên môn. Những người dùng cao cấp hơn có nhiều khả năng chọn mật khẩu 'mạnh', thay đổi chúng thường xuyên, v.v. hơn những người mới sử dụng, có lẽ cho thấy khả năng tiếp xúc

[33] 'Xác thực mật khẩu từ góc độ yếu tố con người: kết quả khảo sát giữa những người dùng cuối', Hoonakker, Bornoe và Carayon, Kỷ yếu Hội nghị thường niên lần thứ 53 của Hiệp hội Nhân tố Con người và Công thái học, tháng 10 năm 2009, www.hfes.org/web/Newsroom/ HFES09-Hoonaker CIS.pdf.

hậu quả của vi phạm an ninh làm tăng mong muốn của mọi người để có được mọi thứ đúng.

Tác động của các biện pháp bảo mật trong việc hạn chế khả năng hoàn thành công việc của người dùng là điều đáng được quan tâm đặc biệt. Tường lửa là một cách hiệu quả để hạn chế ai có thể di chuyển và cái gì, giữa Internet công cộng và mạng nội bộ riêng tư (và hy vọng là an toàn hơn) của một tổ chức. Tuy nhiên, nếu những hạn chế mà họ áp đặt quá nặng nề, thì khả năng ai đó chỉ sao chép tệp vào thẻ nhớ và đi vòng quanh những gì họ coi là chướng ngại vật sẽ tăng lên. Rốt cuộc, mọi người thường được trả lương dựa trên khả năng hoàn thành công việc của họ, chứ không phải dựa trên sự tôn trọng của họ đối với các biện pháp an ninh.

Như các nhà nghiên cứu tại hai trường đại học đã kết luận, 'cần nghiên cứu thêm về mối liên hệ giữa nhận thức về khả năng sử dụng, bảo mật và tiện lợi. Tính hữu ích được cảm nhận, tính dễ sử dụng và sự hài lòng của người dùng quyết định việc sử dụng (đúng) công nghệ, chứ không phải ngược lại'.

Một cách tiếp cận[34] là 'áp dụng cách tiếp cận có sự tham gia để phân tích và thiết kế bảo mật – thu hút sự tham gia của các bên liên quan trong các cuộc thảo luận kỹ thuật và ra quyết định, xung quanh thiết kế bảo mật. Thông qua sự tham gia, các bên liên quan có thể hiểu rõ hơn về các vấn đề bảo mật và có thể truyền đạt nhu cầu bảo mật của chính họ'.

---

[34] 'Lỗ hổng con người trong các hệ thống an ninh', An ninh mạng Nhóm làm việc về nhân tố con người KTN, 2007, http://hornbeam.cs.ucl.ac.uk/hcs/publications/HFWG%20Trắng%20Paper%20Final.pdf.

Lời khuyên hàng đầu ...

Thiết kế phần mềm bảo mật sao cho dễ sử dụng, như một phần của công việc hàng ngày.

Vẫn tốt hơn, lôi kéo người dùng tham gia vào thiết kế của họ.

Đừng tạo cơ hội cho người dùng làm những điều xấu hoặc ngu ngốc.

Giúp người dùng đưa ra lựa chọn tốt.

CHƯƠNG 12: VÀ CUỐI CÙNG...

Nếu bạn chịu trách nhiệm bảo mật thông tin và hệ thống CNTT của tổ chức mình, hãy làm theo năm bước đơn giản sau để đảm bảo các thành viên trong lực lượng lao động của bạn biết chính xác những gì bạn mong đợi ở họ:

Đặt bối cảnh – Đảm bảo rằng mọi người đều biết tại sao bảo mật lại quan trọng đối với tổ chức, khách hàng và công việc của họ. Hãy nói rõ rằng đó là điều CEO muốn họ làm và là điều CEO đang làm cho chính họ.

Đào tạo mọi người – Giải thích rõ ràng và đơn giản những gì bạn muốn mọi người làm và tại sao họ nên làm điều đó. Củng cố thông điệp ở cấp độ nhóm, đảm bảo rằng mọi người đang áp dụng nội dung đào tạo vào công việc hàng ngày của họ. Đưa an ninh vào chương trình thường trực cho các cuộc họp nhóm.

Bảo mật thiết kế – Không chỉ cho các mạng và ứng dụng của bạn, mà còn cho các hệ thống, quy trình và văn hóa của bạn.

Cung cấp dự phòng – Giúp mọi người dễ dàng đặt câu hỏi, báo cáo sự cố và nhận trợ giúp.

Theo dõi, đánh giá và làm mới – Đừng nghỉ ngơi trên vòng nguyệt quế của bạn. Các mối đe dọa mới luôn xuất hiện, mọi người quay trở lại thói quen cũ và việc đào tạo trở nên cũ kỹ. Xác định các biện pháp có ý nghĩa và đa dạng về hiệu suất bảo mật, đánh giá chúng thường xuyên và thực hiện hành động sớm nếu hiệu suất bắt đầu giảm sút.

NGUỒN ITG

Công ty TNHH Quản trị CNTT cung cấp nguồn, tạo và cung cấp các sản phẩm và dịch vụ để đáp ứng nhu cầu quản trị CNTT đang phát triển trong thế giới thực của các tổ chức, giám đốc, nhà quản lý và người hành nghề ngày nay. Trang web ITG (www.itgovernance.co.uk) là cửa hàng quốc tế cung cấp thông tin quản trị công ty và CNTT, tư vấn, hướng dẫn, sách, công cụ, đào tạo và tư vấn.

www.itgovernance.co.uk/it-induction-and-information security.aspx là trang thông tin trên trang web của chúng tôi về các tài nguyên bảo mật thông tin của chúng tôi.

Các trang web khác

Sách và công cụ do IT Governance Publishing xuất bản (ITGP) có sẵn từ tất cả các nhà bán sách kinh doanh và cũng có sẵn ngay lập tức từ các trang web sau:

www.itgovernance.co.uk/catalog/355 cung cấp thông tin và phương tiện mua hàng trực tuyến cho mọi cuốn sách hiện có do ITGP xuất bản.

www.itgovernanceusa.com là một trang web có trụ sở tại US$ cung cấp đầy đủ các sản phẩm Quản trị CNTT cho Bắc Mỹ và vận chuyển từ bên trong lục địa Hoa Kỳ.

www.itgovernanceasia.com cung cấp một loạt sản phẩm ITGP chọn lọc dành riêng cho khách hàng ở Nam Á.

www.27001.com là trang web của IT Governance Ltd liên quan cụ thể đến quản lý bảo mật thông tin và vận chuyển từ bên trong lục địa Hoa Kỳ.

hướng dẫn bỏ túi

Để biết chi tiết đầy đủ về toàn bộ phạm vi hướng dẫn bỏ túi, chỉ cần theo các liên kết www.itgovernance.co.uk/publishing.aspx. Tại

Bộ công cụ

Phạm vi bộ công cụ độc đáo của ITG bao gồm IT
Bộ công cụ Khung quản trị, bao gồm tất cả các công cụ và hướng dẫn mà bạn sẽ cần để phát triển và triển khai khung quản trị CNTT phù hợp cho tổ chức của mình. Chi tiết đầy đủ có thể được tìm thấy tại www.itgovernance.co.uk/products/519.

Để có tài liệu miễn phí về cách sử dụng Khung quản trị CNTT Calder Moir độc quyền và để có phiên bản dùng thử miễn phí bộ công cụ, www.itgovernance.co.uk/calder_moir.aspx. nhìn thấy

Ngoài ra còn có nhiều bộ công cụ để đơn giản hóa việc triển khai các hệ thống quản lý, chẳng hạn như ISO/IEC 27001 ISMS hoặc BS25999 BCMS, và tất cả những bộ công cụ này đều có thể được xem và mua trực tuyến tại: www.itgovernance.co.uk/catalog/1 .

Báo cáo thực tiễn tốt nhất

Phạm vi Báo cáo Thực tiễn Tốt nhất của ITG hiện có tại www.itgovernance.co.uk/best-practice-reports.aspx.
Chúng cung cấp cho bạn thông tin cần thiết, phù hợp, được nghiên cứu chuyên nghiệp về ngày càng nhiều vấn đề chính bao gồm Web 2.0 và CNTT xanh.

Đào tạo và Tư vấn

Quản trị CNTT cũng cung cấp các dịch vụ đào tạo và tư vấn trên toàn bộ các lĩnh vực trong lĩnh vực quản trị thông tin. Chi tiết về các khóa đào tạo có thể truy cập tại www.itgovernance.co.uk/training.aspx

và mô tả về các dịch vụ tư vấn của chúng tôi có thể được

Tài nguyên ITG

tìm thấy tại www.itgovernance.co.uk/consulting.aspx.

Tại sao không liên hệ với chúng tôi để xem làm thế nào chúng tôi có thể giúp bạn và tổ chức của bạn?

bản tin

Quản trị CNTT là một trong những chủ đề nóng nhất trong kinh doanh hiện nay, đặc biệt là vì đây cũng là chủ đề phát triển nhanh nhất, vậy còn cách nào tốt hơn để theo kịp hơn là đăng ký nhận bản tin miễn phí hàng tháng của ITG Sentinel ? Nó cung cấp các bản cập nhật và tài nguyên hàng tháng trên toàn bộ chủ đề quản trị CNTT, bao gồm quản lý rủi ro, bảo mật thông tin, ITIL và quản lý dịch vụ CNTT, quản trị dự án, tuân thủ, v.v.

Đăng ký miễn phí tại www.itgovernance.co.uk/ sao chép Tại: newsletter.aspx của bạn.