The Cybersecurity Campaign Playbook

Nội dung

Chào mừng

Mọi người tham gia các chiến dịch vì những lý do khác nhau: bầu một nhà lãnh đạo mà họ tin tưởng, thúc đẩy chương trình nghị sự, dọn dẹp chính phủ hoặc trải qua sự vội vã và adrenaline của cuộc sống vận động tranh cử. Đây là một số lý do chúng tôi tham gia vào chính trị. Chúng tôi chắc chắn không đăng ký vì chúng tôi muốn trở thành chuyên gia mạng và chúng tôi đoán bạn cũng không đăng ký.

Chúng tôi đến từ các đảng phái chính trị khác nhau và không đồng ý nhiều về chính sách công, nhưng một điều đoàn kết chúng tôi là niềm tin rằng cử tri Mỹ nên quyết định cuộc bầu cử của chúng tôi chứ không phải ai khác. Cách sống và làm việc ngày càng kỹ thuật số của chúng ta cung cấp những cách mới cho các nhà quảng cáo ảnh hưởng đến các chiến dịch và bầu cử của chúng ta. Mặc dù bạn không cần phải là một chuyên gia mạng để thực hiện một chiến dịch thành công, nhưng bạn có trách nhiệm bảo vệ ứng cử viên và tổ chức của mình khỏi các đối thủ trong không gian kỹ thuật số. Đó là lý do tại sao Bảo vệ Dân chủ Kỹ thuật số, một dự án của Trung tâm Khoa học và Các vấn đề Quốc tế Belfer của Trường Harvard Kennedy, đã tạo ra Cẩm nang Chiến dịch An ninh mạng này.

Thông tin được tập hợp ở đây dành cho bất kỳ chiến dịch nào trong bất kỳ đảng nào. Nó được thiết kế để cung cấp cho bạn thông tin đơn giản, có thể hành động sẽ làm cho thông tin chiến dịch của bạn an toàn hơn trước các đối thủ đang cố gắng tấn công tổ chức của bạn — và nền dân chủ của chúng ta

Trên hết, chúng tôi hy vọng tài nguyên này cho phép bạn dành nhiều thời gian hơn cho những gì bạn đã đăng ký — chiến dịch.

Chúc may mắn.

Robby Mook
Hillary Clinton Giám đốc Chiến dịch năm 2016

Matt Rhoades
Mitt Romney Giám đốc chiến dịch năm 2012

Tác giả và Cộng tác viên

Dự án này được thực hiện bởi hàng chục người đã hào phóng tình nguyện dành thời gian của họ.
Xin gửi lời cảm ơn đặc biệt đến **Debora Plunkett** vì đã dẫn dắt dự án và **Harrison Monsky** đã viết tài liệu. Chúng tôi cũng mang ơn những người được liệt kê dưới đây, những người đã đầu tư vô số giờ để xem xét các bản thảo và cung cấp thông tin đầu vào.

Bảo vệ dân chủ kỹ thuật số

Eric Rosenbach, Đồng Giám đốc, Trung tâm Belfer

Robby Mook, Thành viên Trung tâm Belfer

Matt Rhoades, Thành viên Trung tâm Belfer

Heather Adkins, Giám đốc, Bảo mật Thông tin và Quyền riêng tư, Google

Dmitri Alperovitch, Đồng sáng lập và CTO, CrowdStrike

Josh Burek, Giám đốc Truyền thông và Chiến lược Toàn cầu, Trung tâm Belfer

Chris Collins, Đồng sáng lập, First Atlantic Capital

Caitlin Conley, sinh viên, Trường Harvard Kennedy

Mari Dugas, Điều phối viên Dự án, Bảo vệ Dân chủ Kỹ thuật số, Trung tâm Belfer

Josh Feinblum, sinh viên, Học viện Công nghệ Massachusetts

Siobhan Gorman, Giám đốc, Tập đoàn

Brunswick **Stuart Holliday**, Giám đốc điều hành,

Trung tâm Quốc tế Meridian **Dai Lin**, sinh viên,

Trường Harvard Kennedy

Kent Lucken, Giám đốc điều hành, Citibank

Katherine Mansted, sinh viên, Trường Harvard Kennedy

Nicco Mele, Giám đốc, Trung tâm Shorenstein

Debora Plunkett, cựu Giám đốc Đảm bảo Thông tin, Cơ quan An ninh Quốc gia

Jim Routh, Giám đốc An ninh, Aetna

Suzanne E. Spaulding, Cố vấn cao cấp về An ninh Nội địa, Trung tâm Nghiên cứu Chiến lược và Quốc tế

Matthew Spector, sinh viên, Trường Harvard Kennedy

Alex Stamos, Giám đốc bảo mật, Facebook

Phil Venables, Đối tác kiêm Giám đốc Rủi ro Hoạt động, Goldman Sachs

Tác giả và người đóng góp bổ sung

Ryan Borkenhagen,
Giám đốc CNTT, Ủy ban
Chiến dịch Thượng nghị
sĩ Dân chủ

Michael
Chenderlin,
Giám đốc Kỹ
thuật số ,
Definers Public
Affairs

Robert Cohen, Nhà phân tích mối đe

dọa mạng, K2 Intelligence **Julia**

Cotrone, Trợ lý đặc biệt, Definers

Public Affairs **John Flynn**, Giám đốc

An ninh Thông tin, Uber **Daniel**

Griggs, Người sáng lập và Giám đốc

điều hành, cmdSecurity Inc.

Eben Kaplan, Tư vấn chính, CrowdStrike

Greg Kesner, Hiệu trưởng, GDK Consulting

Ryan McGeehan, Thành viên, Bảo mật R10N

Jude Meche, Giám đốc Công
nghệ, Ủy ban Chiến dịch
Thượng nghị sĩ Dân chủ

Eric Metzger,
Đối tác sáng lập
và Giám đốc
điều hành,
cmdSecurity
Inc.

Zac Moffatt, Giám đốc điều hành, Chiến thắng được nhắm
mục tiêu

Harrison Monsky, sinh viên, Trường Luật Harvard

Colin Reed, Phó Chủ tịch Cấp cao,

Definers Public Affairs **Jeff**

Stambolsky, Nhà phân tích phản ứng

bảo mật, CrowdStrike **Frank White**,

Tư vấn Truyền thông Độc lập **Sally**

White, sinh viên, Đại học Harvard

Rob Witoff, Giám đốc bảo mật cấp cao, Google

Nhóm thiết kế và web của Trung tâm Belfer

Arielle Dworkin, Giám đốc
Truyền thông Kỹ thuật số,
Trung tâm Belfer

Andrew Facini, Điều phối viên Xuất
bản và Thiết kế, Trung tâm Belfer

Phương pháp tiếp cận Playbook

Một nhóm chuyên gia lưỡng đảng về an ninh mạng, chính trị và luật đã viết *Cẩm nang Chiến dịch An ninh mạng này* để cung cấp những cách đơn giản, có thể hành động để chống lại mối đe dọa mạng ngày càng tăng.

Kẻ thù mạng không phân biệt đối xử. Các chiến dịch ở tất cả các cấp - không chỉ các chiến dịch tranh cử tổng thống - đã bị tấn công. Bạn nên cho rằng bạn là một mục tiêu. Mặc dù các khuyến nghị trong cẩm nang này áp dụng phổ biến, nhưng nó chủ yếu dành cho các chiến dịch không có nguồn lực để thuê nhân viên an ninh mạng chuyên nghiệp, toàn thời gian. Chúng tôi cung cấp các khối xây dựng cơ bản cho chiến lược giảm thiểu rủi ro an toàn mạng mà những người không được đào tạo kỹ thuật có thể thực hiện (mặc dù chúng tôi bao gồm một số đề xuất cần sự giúp đỡ của chuyên gia CNTT).

Đây là những khuyến nghị cơ bản, *không phải là* tài liệu tham khảo toàn diện để đạt được mức độ bảo mật cao nhất có thể. Chúng tôi khuyến khích tất cả các chiến dịch tranh thủ ý kiến đóng góp chuyên môn từ các chuyên gia CNTT và an ninh mạng có chứng chỉ bất cứ khi nào có thể.

Giới thiệu

Các ứng cử viên và chiến dịch tranh cử phải đối mặt với một loạt thách thức khó khăn. Có những sự kiện để tổ chức, các tình nguyện viên để tuyển dụng, quỹ để gây quỹ và những nhu cầu không ngừng nghỉ của chu kỳ truyền thông hiện đại. Mọi nhân viên phải lường trước những bất ngờ đáng tiếc như sai lầm hoặc quảng cáo tấn công vào phút cuối. Các cuộc tấn công mạng hiện cũng nằm trong danh sách này.

Khi các chiến dịch ngày càng trở nên kỹ thuật số, các đối thủ đã tìm thấy cơ hội mới để can thiệp, phá vỡ và đánh cắp. Năm 2008, tin tặc Trung Quốc đã xâm nhập vào các cam của Obama và McCain, và đánh cắp một lượng lớn thông tin từ cả hai. Năm 2012, các chiến dịch của Obama và Romney đều phải đối mặt với các nỗ lực hack vào mạng và trang web của họ. Năm 2016, các hoạt động mạng được cho là do Nga tài trợ đã đánh cắp và rò rỉ hàng chục nghìn email và tài liệu từ các nhân viên chiến dịch của đảng Dân chủ.

Hậu quả của một vụ vi phạm mạng có thể rất lớn. Tin tức về một vụ vi phạm, kết hợp với việc tiết lộ thông tin bị đánh cắp chậm rãi, có thể làm trật bánh thông điệp của ứng cử viên trong nhiều tháng. Những kẻ tấn công làm quá tải một trang web có thể dẫn đến mất các khoản quyên góp vào những thời điểm quan trọng. Việc đánh cắp dữ liệu cá nhân của nhà tài trợ có thể tạo ra trách nhiệm pháp lý đáng kể và khiến các nhà tài trợ miễn cưỡng đóng góp vào một cam kết. Các cuộc tấn công phá hoại nhắm vào máy tính của nhân viên hoặc máy chủ chiến dịch quan trọng có thể làm chậm hoạt động của chiến dịch trong nhiều ngày hoặc thậm chí vài tuần. Dọn dẹp mớ hỗn độn kết quả sẽ chuyển hướng các nguồn tài nguyên quý giá trong sức nóng của một cuộc đua sát sao, cho dù đó là cho tổng thống hay hội đồng thành phố.

Trong tương lai gần, các mối đe dọa mạng sẽ vẫn là một phần thực sự trong quá trình vận động tranh cử của chúng tôi. Là tiền tuyến của nền dân chủ, nhân viên chiến dịch phải nhận ra nguy cơ của một cuộc tấn công, phát triển một chiến lược để giảm rủi ro đó càng nhiều càng tốt và thực hiện các chiến lược ứng phó cho thời điểm điều tồi tệ nhất xảy ra. Mặc dù không có chiến dịch nào có thể đạt được bảo mật hoàn hảo, nhưng thực hiện một vài bước đơn giản có thể khiến *các tác nhân độc hại khó gây hại hơn nhiều*. Trớ trêu thay, nhà nước tinh vi nhất
Các tác nhân thường chọn các phương pháp tấn công ít tinh vi nhất, săn mồi vào con người và tổ chức những người bỏ qua các giao thức bảo mật cơ bản. Đó là lý do chính của chúng tôi để tạo ra *Cẩm nang Chiến dịch An ninh mạng* này.

Trong các chiến dịch ngày nay, an ninh mạng là *trách nhiệm của mọi người*. Lỗi của con người luôn là nguyên nhân gốc rễ của các cuộc tấn công mạng được công khai, và tùy thuộc vào ứng cử viên và các nhà lãnh đạo chiến dịch để đưa nhận thức về bảo mật vào văn hóa của tổ chức. *Các quyết định mà con người đưa ra cũng quan trọng như phần mềm họ sử dụng.* Trong tương lai, các chiến dịch tốt nhất sẽ có các tiêu chuẩn rõ ràng về làm việc chăm chỉ, duy trì thông điệp, trung thành với nhóm — và tuân theo giao thức bảo mật tốt.

Trước khi chúng ta đi vào các khuyến nghị của mình, chúng ta hãy nhanh chóng đóng khung vấn đề:

- môi **trường** mà chiến dịch của bạn đang hoạt động;
- các **mối đe dọa mà** chiến dịch của bạn có thể phải đối mặt; và,
- tầm **quan trọng** của quản lý rủi ro mạng.

Môi trường chiến dịch dễ bị tổn thương

Các chiến dịch ngày nay là những mục tiêu mềm độc đáo. Chúng vốn dĩ là tạm thời và thoáng qua. Họ không có thời gian hoặc tiền bạc để phát triển các chiến lược bảo mật dài hạn, đã được kiểm tra kỹ lưỡng. Một số lượng lớn nhân viên mới thường được tuyển dụng nhanh chóng mà không cần nhiều thời gian đào tạo. Họ có thể mang theo phần cứng của riêng mình từ nhà và phần mềm độc hại ẩn nấp trên đó. Các sự kiện diễn ra nhanh chóng, rủi ro cao và mọi người cảm thấy rằng họ không có thời gian để quan tâm đến an ninh mạng. Có rất nhiều cơ hội để có điều gì đó không ổn.

Đồng thời, các chiến dịch ngày càng dựa nhiều vào thông tin độc quyền về cử tri, nhà tài trợ và dư luận. Họ cũng lưu trữ các tài liệu nhạy cảm như nghiên cứu đối lập, nghiên cứu về tính dễ bị tổn thương, tài liệu kiểm tra nhân sự, tài liệu chính sách dự thảo đầu tiên và email trên các máy chủ khác nhau. Rủi ro của một cuộc tấn công tiềm ẩn đang tăng lên và hậu quả cũng vậy.

SỰ NGUY HIỂM CỦA MỘT CUỘC TẤN CÔNG:

Hãy hình dung điều này: Một tháng trước Ngày Bầu cử, và cuộc đua rất chặt chẽ. Bạn đến trụ sở sớm, bật máy pha cà phê, đến bàn làm việc và đăng nhập vào máy tính của bạn. Một màn hình đen bật lên, sau đó là một bức tranh biếm họa khủng khiếp về ứng cử viên của bạn, tiếp theo là một tin nhắn. Ổ cứng của bạn đã được xóa sạch. Mọi thông tin kỹ thuật số mà bạn thu thập được - bản ghi nhớ, danh sách nhắm mục tiêu, bảng cân đối kế toán - đều biến mất. Bạn đọc, lấy lại nó sẽ tiêu tốn một triệu Bitcoin tuyệt vời và từ bỏ một vị trí chính sách quan trọng.

Một nhóm không xác định đã xâm nhập vào máy tính của bạn vài tháng trước và đã âm thầm đánh cắp email, bản ghi nhớ chiến lược, địa chỉ của các nhà tài trợ và số An sinh xã hội của nhân viên. Nhóm đã dành nhiều tuần để lùng sục tiền thưởng để tìm kiếm đồ giặt bẩn và tạo ra một trang web dễ sử dụng chỉ dành riêng cho việc phân phối những điểm nổi bật. Nổi bật là một cuốn sách "tự nghiên cứu" dài về ứng viên của bạn. Hiện tại, trang web của chiến dịch đã ngừng hoạt động, các tài khoản mạng xã hội của nó đã bị đình chỉ vì đưa ra những hình ảnh dâm dục và không có

Các mối đe dọa mà các chiến dịch phải đối mặt

Thật không may cho các chiến dịch và đất nước của chúng ta, các đối thủ nước ngoài có thể nghĩ rằng làm hại hoặc giúp đỡ một ứng cử viên cụ thể thúc đẩy lợi ích quốc gia của họ, cho dù điều đó có nghĩa là tạo ra sự hỗn loạn và nhầm lẫn trong cử tri Mỹ, hoặc trừng phạt một quan chức đã lên tiếng chống lại họ. Điều này nghe có vẻ giống như viễn tưởng kinh dị, nhưng thực tế là một cơ quan tình báo nước ngoài tinh vi, tội phạm mạng hoặc hacktivist có mối hận thù với một ứng cử viên, có thể quyết định rằng bạn hoặc ai đó trong chiến dịch của bạn là mục tiêu.

Đây là những loại mối đe dọa mà các nhà quản lý và nhân viên phải nhận ra là có thể xảy ra.

AI ĐANG HACK?

Các chiến dịch phải đối mặt với các mối đe dọa thông tin và an ninh mạng từ nhiều tác nhân. Tin tặc và tội phạm mạng "mũ đen" đơn độc đã cố gắng thỏa hiệp các chiến dịch vì lý do lợi ích cá nhân, tai tiếng hoặc mong muốn đơn giản là xem liệu họ có thể làm được hay không. Các quốc gia dân tộc đặt ra mối đe dọa tận tụy và dai dẳng nhất. Các nhóm gián điệp của Nga được gọi là "Fancy Bear" (APT 28) và "Cozy Bear" (APT 29) có liên quan đến các vụ hack chiến dịch năm 2016. Người Trung Quốc đã tập trung nhiều hơn vào việc thu thập thông tin. Họ được cho là đã hoạt động tích cực trong các chiến dịch tranh cử tổng thống năm 2008 và 2012, nhưng không có bằng chứng nào cho thấy họ đã tiết lộ bất kỳ tài liệu bị đánh cắp nào. Triều Tiên đã trả đũa Sony Pictures Entertainment vì đã sản xuất bộ phim The *Interview* bằng cách đánh cắp và phát hành email của công ty và xóa sạch hệ thống của họ. Căng thẳng gia tăng

Quản lý rủi ro mạng

Rủi ro được hiểu rõ nhất trong hai phần. Đầu tiên, có những ***lỗ hổng***: điểm yếu trong chiến dịch của bạn khiến thông tin dễ bị đánh cắp, thay đổi hoặc phá hủy. Các lỗ hổng có thể bắt nguồn từ phần cứng, phần mềm, quy trình và mức độ cảnh giác của nhân viên của bạn. Sau đó là các ***mối đe dọa*** thực sự: các quốc gia dân tộc, hacktivist và các nhóm phi nhà nước khác có khả năng khai thác các lỗ hổng đó. Rủi ro phát sinh khi mối đe dọa và lỗ hổng gặp nhau.

Bạn hoặc chiến dịch của bạn có thể làm rất ít để ngăn chặn các mối đe dọa – chúng là kết quả của các lực lượng địa chính trị, kinh tế và xã hội lớn hơn. Những gì bạn *có thể* làm là giảm đáng kể khả năng đối thủ của bạn sẽ thành công bằng cách giảm tính dễ bị tổn thương của chính bạn. Giảm
Tính dễ bị tổn thương làm giảm rủi ro — tùy thuộc vào bạn để quyết định cái nào là cần thiết nhất để giải quyết. Ví dụ, bạn có thể quyết định rằng điều gây hại nhất mà tin tặc có thể làm là đánh cắp báo cáo tự nghiên cứu của ứng cử viên của bạn. Để đáp lại, bạn dành thêm tài nguyên cho lưu trữ dựa trên đám mây an toàn, sử dụng xác thực hai yếu tố và hạn chế quyền truy cập đối với một số lượng nhỏ người. Bạn có thể quyết định làm cho các tài liệu khác về chiến dịch có sẵn rộng rãi hơn và kém an toàn hơn, vì nhiều người cần chúng để thực hiện công việc của họ và chúng sẽ không gây ra nhiều thiệt hại nếu chúng bị rò rỉ.

Có những khía cạnh kỹ thuật để giảm thiểu rủi ro, nhưng điều quan trọng nhất là bạn thực hiện một cách tiếp cận toàn diện. Là một nhà lãnh đạo chiến dịch, bạn phải đưa ra những lựa chọn cơ bản, chẳng hạn như ai có quyền truy cập vào thông tin, thông tin nào được giữ lại hoặc loại bỏ, bạn dành bao nhiêu thời gian cho đào tạo bảo mật và cách bạn cư xử như một hình mẫu. Là một chuyên gia chiến dịch, quản lý rủi ro là
trách nhiệm của bạn — cả kỹ thuật và con người. Tùy thuộc vào bạn để quyết định dữ liệu và hệ thống nào có giá trị nhất và bạn cam kết tài nguyên nào để bảo vệ chúng.

Bảo mật chiến dịch của bạn

Các đề xuất bảo mật của chúng tôi được sắp xếp theo ba nguyên tắc:

Chuẩn bị

Sự thành công của gần như mọi khuyến nghị *của Playbook* phụ thuộc vào việc người quản lý chiến dịch tạo ra một văn hóa cảnh giác bảo mật để giảm thiểu các liên kết yếu. Điều đó có nghĩa là thiết lập các quy tắc cơ bản rõ ràng được thực thi từ trên xuống và được chấp nhận từ dưới lên.

Bảo vệ

Bảo vệ là rất quan trọng. Khi bạn phát hiện ra mình gặp vấn đề bảo mật, thì đã quá muộn. Xây dựng hệ thống phòng thủ mạnh nhất mà thời gian và tiền bạc cho phép là chìa khóa để giảm rủi ro. Internet và bảo mật dữ liệu hoạt động tốt nhất theo lớp: không có công nghệ hoặc sản phẩm duy nhất, chống đạn. Một vài biện pháp cơ bản được sử dụng kết hợp có thể làm cho kiến trúc kỹ thuật số của chiến dịch khó vi phạm hơn và có khả năng phục hồi hơn nếu bị xâm phạm.

Tồn tại

Các chiến dịch hiện phải đối mặt với các đối thủ với mức độ tài nguyên và kinh nghiệm ngày càng tăng; Ngay cả văn hóa cảnh giác nhất và cơ sở hạ tầng cứng rắn nhất cũng có thể không ngăn chặn được vi phạm bảo mật. Các chiến dịch cần phát triển một kế hoạch trước thời hạn để đối phó với một vi phạm nếu xảy ra.

Một số chiến dịch có nhiều thời gian và tiền bạc hơn cho an ninh mạng so với những chiến dịch khác. Đó là lý do tại sao các đề xuất của chúng tôi cung cấp hai cấp độ bảo vệ: "**tốt**" và "**nâng cao**". Cấp "tốt" đại diện cho mọi thứ mà một chiến dịch ***phải*** làm để có mức độ bảo mật ***tối thiểu***. Sử dụng các đề xuất "tốt" một cách từng phần sẽ khiến bạn dễ bị tổn thương. Bạn nên luôn khao khát làm được nhiều hơn khi thời gian, tiền bạc và con người cho phép, đó là lý do tại sao chúng tôi khuyên bạn nên sử dụng cấp độ "nâng cao" bất cứ khi nào có thể. Nếu bạn có đủ nguồn lực để nhận được hỗ trợ CNTT uy tín, được đào tạo, thì đó là số tiền được chi tiêu xứng đáng. Các mối đe dọa không ngừng phát triển và các dịch vụ CNTT chuyên nghiệp sẽ giúp bạn vượt xa những gì cẩm nang này cung cấp và giúp bạn cập nhật các mối đe dọa và giải pháp mới nhất.

Sự quản lý

Các nhà quản lý chiến dịch cần phải chịu trách nhiệm về chiến lược an ninh mạng của họ, nhưng hầu hết sẽ giao việc phát triển và giám sát cho một phó hoặc giám đốc điều hành. Điều quan trọng là an ninh mạng phải được tích hợp chặt chẽ vào công việc nhân sự và CNTT, vì việc giới thiệu nhân viên, cung cấp phần cứng và kiểm soát quyền một cách chính xác sẽ rất quan trọng đối với chiến lược của bạn. Nhiều chiến dịch nhỏ sẽ dựa vào sự hỗ trợ tình nguyện cho CNTT và an ninh mạng. Bạn có thể sử dụng cẩm nang này để hướng dẫn cuộc thảo luận của mình với sự hỗ trợ tình nguyện của bạn. Điều quan trọng là kiểm tra cẩn thận các tình nguyện viên hỗ trợ bạn và kiểm soát cẩn thận quyền truy cập, để hỗ trợ tình nguyện viên không tạo ra các lỗ hổng mới. Bạn nên đảm bảo rằng nhân viên chiến dịch đang giám sát công việc CNTT và kiểm soát quyền truy cập vào các hệ thống khác nhau.

Khi nào bắt đầu

Dù bạn có mô hình hỗ trợ nào, *an ninh mạng nên bắt đầu ngay từ ngày đầu tiên*. Những gì sau đây là "danh sách kiểm tra hàng đầu" của các biện pháp hoàn toàn quan trọng. Đảm bảo rằng những điều này được thực hiện ngay từ đầu, ngay cả khi chỉ có một hoặc hai nhân viên, sau đó hoàn thành các khuyến nghị "tốt" khác càng sớm càng tốt.

Chi phí

Rất nhiều điều chúng tôi đề xuất ở đây là miễn phí hoặc chi phí rất thấp. Trên thực tế, mọi thứ trong danh sách top 5 của chúng tôi đều miễn phí, ngoại trừ việc mua một nền tảng dựa trên đám mây, sẽ chỉ tốn vài đô la mỗi tháng cho mỗi nhân viên. Các chiến dịch có mục tiêu cao sẽ cần ngân sách đủ nguồn lực cho phần cứng và phần mềm để thực hiện một chiến lược có trách nhiệm, nhưng đây vẫn phải là một tỷ lệ rất nhỏ trong ngân sách chiến dịch hàng triệu đô la trên toàn tiểu bang. Các chiến dịch nhỏ hơn sẽ có thể thực hiện các đề xuất ở đây với giá vài trăm đến vài nghìn đô la tùy thuộc vào số lượng nhân viên hoặc tình nguyện viên làm việc trong chiến dịch.

Mọi tham chiếu đến nhà cung cấp và sản phẩm nhằm giúp cung cấp ví dụ về các giải pháp phổ biến, nhưng không cấu thành xác nhận. Nếu gặp khó khăn khi triển khai sản phẩm hoặc dịch vụ, chúng tôi khuyến khích bạn liên hệ trực tiếp với các nhà cung cấp, những người thường có thể cung cấp hỗ trợ kỹ thuật ở cấp độ người dùng. Khi nói đến việc lựa chọn sản phẩm và dịch vụ, chúng tôi khuyến khích mọi chiến dịch tham khảo ý kiến của chuyên gia an ninh mạng hoặc tiến hành nghiên cứu độc lập để tìm ra sản phẩm tốt nhất cho nhu cầu của họ.

Danh sách kiểm tra năm bước

1. Đặt trọng tâm:

Hãy coi trọng an ninh mạng. Chịu trách nhiệm giảm thiểu rủi ro, đào tạo nhân viên của bạn và làm gương. Lỗi của con người là nguyên nhân số một của vi phạm.

(xem trang 12)

2. Sử dụng đám mây dịch vụ:

Một dịch vụ đám mây lớn, thương mại sẽ an toàn hơn nhiều so với bất kỳ thứ gì bạn có thể thiết lập. Sử dụng bộ ứng dụng văn phòng dựa trên đám mây như GSuite hoặc Microsoft365 sẽ cung cấp tất cả các chức năng văn phòng cơ bản của bạn và một nơi an toàn để lưu trữ thông tin. *(xem trang 14-15)*

3. Sử dụng xác thực hai yếu tố (2FA):

Yêu cầu 2FA cho tất cả các tài khoản quan trọng, bao gồm bộ ứng dụng văn phòng, bất kỳ dịch vụ email hoặc lưu trữ nào khác và tài khoản mạng xã hội của bạn. Sử dụng ứng dụng di động hoặc khóa vật lý cho yếu tố thứ hai của bạn, không phải nhắn tin văn bản. *(xem trang 16-17)*

4. Tạo mật khẩu mạnh, dài:

Đối với mật khẩu của bạn, hãy tạo `SOMETHINGREALLYLONGLIKETHISSTRING`, không phải một cái gì đó thực sự ngắn như `Th1$`. Trái ngược với suy nghĩ của nhiều người, một chuỗi dài các từ ngẫu nhiên không có ký hiệu khó phá vỡ hơn một từ ngắn, với L0t$ 0f $ymB 01$. Trình quản lý mật khẩu cũng có thể trợ giúp.

(xem trang 17)

5. Lập kế hoạch và chuẩn bị:

Có kế hoạch trong trường hợp bảo mật của bạn bị xâm phạm. Biết ai cần gọi trợ giúp kỹ thuật, hiểu nghĩa vụ pháp lý của bạn và sẵn sàng giao tiếp nội bộ và bên ngoài nhanh nhất có thể.

(xem trang 19-22)

Các bước để bảo mật chiến dịch của bạn

Bước 1: Yếu tố con người

An ninh mạng về cơ bản là vấn đề của con người, không phải là vấn đề kỹ thuật. Các giải pháp công nghệ tốt nhất trên thế giới sẽ không có tác dụng nếu chúng không được thực hiện đúng cách, hoặc nếu chúng không được cập nhật liên tục khi công nghệ phát triển. Các hoạt động an ninh mạng thành công phụ thuộc vào việc tạo ra văn hóa nhận thức về bảo mật.

"Tốt" - Những gì bạn cần làm

1. **Thiết lập văn hóa bảo mật thông tin mạnh mẽ** , nhấn mạnh bảo mật như một tiêu chuẩn cho một chiến dịch thành công. Cũng giống như các nhân viên chiến dịch được hướng dẫn không được quyên góp bất hợp pháp, nhân viên nên biết tránh nhấp vào liên kết hoặc mở tệp đính kèm trong email từ những người gửi không xác định.

    a. **Giới thiệu: Cung cấp** đào tạo bảo **mật thông tin cơ bản** khi bạn giới thiệu nhân viên mới. Bạn có thể phân phát Tài *liệu cho Nhân viên* tại khóa đào tạo của mình.

    b. **Đào tạo:** Biến an ninh thành một phần của tất cả các **khóa đào tạo nhân viên đang diễn ra của bạn,** chẳng hạn như khóa tu của nhân viên cấp cao hoặc đào tạo GOTV. Cung cấp **đào tạo bổ sung** cho những người có vai trò nhạy cảm, chẳng hạn như ứng viên, nhân viên báo chí, nhân viên cấp cao và bất kỳ ai có đặc quyền quản trị hệ thống trên mạng của bạn. Các nhà quản lý nên yêu cầu những người quan trọng nhất trong chiến dịch - bao gồm cả ứng cử viên - phải kiểm tra cài đặt bảo mật của họ bởi bất kỳ ai điều hành CNTT (đó có thể là chính người quản lý). Đừng rụt rè hoặc nửa vời về an ninh cho ứng viên và các VIP khác!

    c. **Đặt ví dụ:** Nhân viên chiến dịch cấp cao và ứng cử viên phải đóng vai **trò lãnh đạo rõ ràng,** ủng hộ an ninh mạng trong các khóa đào tạo. Nhân viên cấp cao nên định **kỳ củng cố** tầm quan trọng của an ninh mạng cho nhân viên cấp dưới trong các cuộc họp và cuộc gọi. Đừng chỉ để các chuyên gia kỹ thuật tiến hành đào tạo. Người quản lý chiến dịch hoặc giám đốc điều hành có thể là một người đưa tin mạnh mẽ hơn chính xác vì họ được coi là ít "kỹ thuật" hơn.

2. **Tiến hành kiểm tra kỹ lưỡng nhân viên, tình nguyện viên và thực tập sinh** — bất kỳ ai yêu cầu quyền truy cập vào thông tin chiến dịch — để tránh cung cấp thông tin đăng nhập cho ai đó muốn đánh cắp hoặc phá hoại hệ thống của bạn. Thiết lập định nghĩa cho **thông tin nhạy cảm** và quy tắc sử dụng thông tin đó. Ví dụ: bạn có thể chọn phân loại tất cả các cuộc thăm dò ý kiến, tài liệu

nghiên cứu, bản ghi nhớ chiến lược và email liên quan là "nhạy cảm". Cấm truyền thông tin nhạy cảm trên các kênh liên lạc không được quản lý và bảo mật

bởi chiến dịch. Bạn có thể yêu cầu chỉ chuyển thông qua tin nhắn được mã hóa (xem Bước 2).

3. **Xác nhận rằng các nhà tư vấn và nhà cung cấp có quyền truy cập vào thông tin nhạy cảm có email và bộ nhớ an toàn** (xem Bước 2). Khi nghi ngờ, hãy yêu cầu các nhà cung cấp và chuyên gia tư vấn sử dụng tài khoản trên bộ ứng dụng văn phòng dựa trên đám mây của bạn (Xem Bước 2).

4. **Kiểm soát quyền truy cập vào** các dịch vụ trực tuyến quan trọng, chẳng hạn như tài khoản mạng xã hội chính thức của chiến dịch, để ngăn chặn việc sử dụng bởi các cá nhân trái phép. Đảm bảo rằng những người rời khỏi chiến dịch không thể truy cập vào các tài khoản liên quan đến chiến dịch nữa. Bạn có thể làm điều này một cách dễ dàng bằng cách sử dụng công cụ quản lý tài khoản mạng xã hội hoạt động như một cổng vào tất cả các tài khoản của bạn. Nếu ai đó rời khỏi chiến dịch, bạn nên tắt ngay tài khoản của họ.

5. **Giáo dục nhân viên về mối đe dọa lừa đảo**. Đảm bảo rằng họ biết cách phát hiện và tránh các liên kết đáng ngờ, đồng thời nhấn mạnh tầm quan trọng của việc xác định và báo cáo các cuộc tấn công lừa đảo tiềm ẩn. Là một phần của văn hóa bảo mật mạnh mẽ của chiến dịch, nhân viên cấp cao nên công nhận và khen ngợi bất kỳ ai báo cáo hành vi đáng ngờ trên hệ thống của họ hoặc thừa nhận nhấp vào một liên kết độc hại tiềm ẩn.

"Nâng cao" - Thực hiện bước tiếp theo

1. Các sản phẩm phần mềm như Phishme và KnowBe4 có thể **đào tạo nhân viên của bạn bằng cách gửi cho họ các email lừa đảo giả mạo**. Đây là một cách an toàn, nhanh chóng và hiệu quả để tìm hiểu ai có nguy cơ nhấp vào liên kết, vì vậy bạn có thể tư vấn và đào tạo thêm cho họ. Nhiều sản phẩm trong số này cũng lọc một số nỗ lực lừa đảo ra khỏi email của bạn.

2. Nếu bạn có nguồn lực, hãy **thuê một chuyên gia CNTT chuyên dụng** để quản lý hệ thống chiến dịch của bạn và một chuyên gia bảo mật CNTT để giúp bảo vệ, duy trì và giám sát cơ sở hạ tầng kỹ thuật số của chiến dịch của bạn. Họ có thể cung cấp đào tạo bảo mật thường xuyên và kiểm tra con người và hệ thống của bạn, đồng thời tùy chỉnh các giải pháp bảo mật.

3. Hợp đồng với một **công ty an ninh mạng** để cung cấp các giải pháp bảo mật, xem xét các biện pháp phòng thủ của bạn và / hoặc giám sát hệ thống của bạn để phát hiện vi phạm. Biết bạn muốn liên hệ với công ty nào nếu bạn bị vi phạm và cần hỗ trợ ứng phó sự cố khẩn cấp. Đây là một giải pháp thay thế cho việc thuê một chuyên gia bảo mật CNTT toàn thời gian. Hãy nghiên cứu và đi với một công ty có uy tín cao, có trụ sở tại Hoa Kỳ — không phải tất

cả các công ty an ninh mạng đều cung cấp cùng một mức độ dịch vụ.

LÀM VIỆC VỚI CÁC CHUYÊN GIA BẢO MẬT

Nếu bạn quyết định làm việc với một chuyên gia bảo mật, bạn sẽ đánh giá đúng người hoặc công ty như thế nào? Cho dù đó là thông qua các đề xuất cá nhân hay đánh giá tích cực của công chúng,
Điều quan trọng là bạn phải tránh hỗ trợ tốn kém nhưng không hiệu quả. Khi phỏng vấn các chuyên gia bảo mật tiềm năng, hãy hỏi về cách họ đã phản ứng với các sự cố bảo mật trong quá khứ và cách họ đã giúp những người khác làm việc an toàn hơn. Ủy ban đảng quốc gia tương ứng của bạn hoặc các chuyên gia chiến dịch đáng tin cậy có thể đề xuất các lựa chọn
để lựa chọn. Hãy nhớ rằng văn hóa ảnh hưởng đến bảo mật và ngay cả những khuyến nghị tốt nhất cũng có thể không đạt được kết quả nếu chúng không

Bước 2: Giao tiếp

Không phải tất cả các phương thức giao tiếp đều an toàn như nhau, vì vậy hãy sử dụng phương pháp an toàn nhất có thể. Lãnh đạo chiến dịch nên đặt ra một tiêu chuẩn khuyến khích các cuộc trò chuyện trực tiếp bất cứ khi nào có thể và không khuyến khích các email không cần thiết hoặc thừa thãi.
Cho dù đó là cuộc gọi điện thoại, nhắn tin hay gửi email, các sản phẩm và dịch vụ khác nhau cung cấp các mức độ bảo vệ khác nhau, vì vậy hãy nghiên cứu trước khi chọn hệ thống mà chiến dịch của bạn sẽ sử dụng.

"Tốt" - Những gì bạn cần làm

1. **Sử dụng bộ ứng dụng văn phòng dựa trên đám mây** cung cấp giao tiếp email an toàn, tạo tài liệu, trò chuyện và chia sẻ tệp, chẳng hạn như GSuite hoặc Microsoft365. Ví dụ: GSuite bao gồm Google Drive để chia sẻ tệp, Gmail để lưu trữ email, Google Hangouts để trò chuyện và Google Tài liệu để xử lý văn bản, bảng tính và bản trình bày. Microsoft365 cung cấp OneDrive/SharePoint để chia sẻ tệp, Outlook/Exchange cho email, Microsoft Teams để trò chuyện và Microsoft Office để xử lý văn bản, bảng tính và bản trình bày. Các hệ thống dựa trên đám mây do các công ty lớn quản lý sẽ được bảo vệ tốt hơn bất kỳ máy chủ nào bạn có thể thiết lập trong chiến dịch của mình. Có phiên bản miễn phí của cả hai sản phẩm, nhưng phiên bản trả phí cung cấp cho bạn
nhiều khả năng quản trị khác. Google cũng cung cấp một dịch vụ có tên là *Bảo vệ Bầu cử của Quý vị* sẽ cung cấp thêm khả năng bảo vệ chống lừa đảo cho dịch vụ email miễn phí của họ. Họ cũng cung cấp một dịch vụ miễn phí để bảo vệ trang

web của bạn khỏi các cuộc tấn công vô hiệu hóa.

ĐÁM MÂY LÀ GÌ?

"Dịch vụ đám mây" cung cấp quản lý và truy cập vào thông tin được lưu trữ từ xa trên Internet. Chúng chạy trên các máy chủ bên ngoài do các công ty bên thứ ba quản lý; điều này bao gồm nhiều dịch vụ phổ biến mà bạn có thể đã sử dụng, chẳng hạn như Gmail hoặc Dropbox.

Thật tốt khi lưu trữ thông tin trên đám mây thay vì trên máy tính cá nhân của bạn vì các nhà cung cấp đám mây lớn có tiền và chuyên môn để làm cho các trang trại máy chủ của họ an toàn hơn ổ cứng máy tính xách tay của bạn hoặc máy chủ văn phòng. **Nó giống như sự khác biệt giữa việc để tiền mặt dưới nệm của bạn và cất nó trong kho bảo mật của ngân hàng.**Sử dụng các dịch vụ đám mây cung cấp một biện pháp hỗ trợ bổ sung chống mất dữ liệu nếu một thiết bị riêng lẻ bị mất hoặc bị xâm phạm. Lưu trữ đám mây là một tính năng đi kèm

2. **Sử dụng các hệ thống an toàn nhất có thể để** liên lạc**.**

    a. **Sử dụng các dịch vụ nhắn tin được mã hóa** như Signal, Wickr, đặc biệt là cho tin nhắn, chia sẻ tài liệu và cuộc gọi điện thoại. Nhiều chiến dịch yêu cầu thông tin nhạy cảm *chỉ được* truyền bằng tin nhắn được mã hóa, mặc dù bạn có thể sử dụng nó cho tất cả các giao tiếp nếu bạn muốn (điều này đặc biệt thông minh đối với những cá nhân có nguy cơ cao như ứng viên). Signal và Wickr cho phép bạn tự động xóa tin nhắn, giúp giảm rủi ro.

    b. **Tắt tính năng lưu trữ cho các dịch vụ nhắn tin**, chẳng hạn như Google Chat và Slack, để các cuộc trò chuyện cũ không thể bị đánh cắp sau này. Điều này yêu cầu đi vào "cài đặt" và điều chỉnh các mốc thời gian "chính sách lưu giữ". Một số dịch vụ yêu cầu bạn làm điều này cho mọi cuộc trò chuyện. Chúng tôi khuyên bạn nên giữ lại tin nhắn trò chuyện trong một tuần hoặc ít hơn.

3. **Bảo vệ email của bạn**

    a. **Bật Tự động xóa** trong ứng dụng email của bạn cho các email cũ để giảm số lượng email có khả năng bị đánh cắp. Điều này thường yêu cầu đi vào và thay đổi "Chính sách lưu giữ" thành khoảng thời gian ngắn hơn trong "Cài đặt". Để đảm bảo email không chỉ nằm trong thư mục "mục đã xóa", hãy điều chỉnh cài đặt để tự động xóa thư mục "mục đã xóa" sau một khoảng thời gian nhất định. Chúng tôi khuyên bạn nên giữ lại email trong một tháng hoặc ít hơn.

4. **Bảo mật tài khoản cá nhân**

    a. **Hoạt động kinh doanh chiến dịch không bao giờ nên đi trên tài khoản cá nhân**. Tuy nhiên, kẻ thù sẽ nhắm mục tiêu tài khoản cá nhân để hack, vì vậy hãy yêu cầu nhân viên của bạn sử dụng mật khẩu mạnh và hai yếu tố cho tài khoản cá nhân của họ (điều này có trong Tài *liệu phát tay nhân viên* của chúng tôi).

MÃ HÓA LÀ GÌ?

Mã hóa là một cách mã hóa thông tin khi nó di chuyển giữa những người dùng hoặc khi nó được lưu trữ, vì vậy nó không thể được đọc bởi bất kỳ ai ngoại trừ người nhận dự định. Hãy nghĩ theo cách này: người dùng "xáo trộn" dữ liệu khi cô ấy gửi dữ liệu và chỉ người nhận dự định mới có chìa khóa để giải mã dữ liệu đó. Sử dụng mã hóa là thông minh, đặc biệt là đối với thông tin nhạy cảm, bởi vì ngay cả khi kẻ thù đánh cắp dữ liệu, chúng cũng không có khả năng đọc được dữ liệu đó. Hầu hết các ứng dụng sử dụng mã hóa, như Signal hoặc Wickr, làm cho quá trình này trở nên liền mạch. Máy tính xách tay hoặc hệ thống lưu trữ đám mây cũng sử dụng mã hóa.

Bước 3: Truy cập và quản lý tài khoản

Một trong những khía cạnh thách thức nhất của bảo mật là ngăn chặn những người không được phép. Điều này có nghĩa là ngăn chặn đối thủ truy cập vào dữ liệu của bạn *và* ngăn chặn những người trong chiến dịch của bạn có quyền truy cập vào thông tin mà họ không cần. Mặc dù một số khuyến nghị dưới đây có vẻ cồng kềnh, nhưng tin tặc phụ thuộc vào những người coi trọng sự tiện lợi hơn bảo mật.

"Tốt" - Những gì bạn cần làm

1. **Yêu cầu xác thực hai yếu tố (2FA)** trên tất cả các hệ thống và ứng dụng. **Tránh nhắn tin (SMS)** để xác thực hai yếu tố, vì kẻ tấn công có thể dễ dàng sao chép số điện thoại và truy cập vào tin nhắn. Có một số ứng dụng 2FA hoạt động tốt như nhắn tin, chẳng hạn như Google Authenticator, Microsoft Authenticator và Duo Mobile. Bạn cũng có thể sử dụng khóa FIDO ("nhận dạng nhanh trực tuyến") vật lý được cắm vào ổ USB của mình như Yubikey hoặc Feitian. Trang web "TwoFactorAuth.org" là một hướng dẫn hữu ích về các dịch vụ có và không cung cấp 2FA.

XÁC THỰC HAI YẾU TỐ LÀ GÌ?

Xác thực hai yếu tố là lớp bảo mật thứ hai yêu cầu người dùng cung cấp thêm thông tin đăng nhập ngoài mật khẩu của họ. Yếu tố thứ hai rất quan trọng vì nếu mật khẩu của bạn bị đánh cắp, kẻ thù vẫn không thể đăng nhập vào tài khoản của bạn. Mật khẩu của bạn là thứ bạn *biết* và yếu tố thứ hai của bạn là thứ bạn *có,* chẳng hạn như mã được tạo bởi một ứng dụng, một khóa vật lý hoặc thậm chí là thứ gì đó sinh trắc học, chẳng hạn như dấu vân tay.

2. **Mật khẩu**

    a. **Yêu cầu mật khẩu mạnh**. Như chúng tôi đã lưu ý trước đó, "tạo mật khẩu dài và mạnh". Khả năng tính toán hiện tại có thể bẻ khóa mật khẩu bảy ký tự trong mili giây. Mật khẩu 20 hoặc thậm chí 30 ký tự sẽ mất nhiều thời gian hơn để tin tặc bẻ khóa. Chọn một chuỗi từ mà bạn có thể dễ dàng nhớ.

    b. **Sử dụng một mật khẩu khác cho các tài khoản khác nhau** để tin tặc không thể xâm nhập vào nhiều tài khoản nếu một mật khẩu bị đánh cắp.

    c. **Nếu ai đó liên hệ yêu cầu đặt lại mật khẩu** hoặc mật khẩu, hãy yêu cầu yêu cầu được thực hiện trực tiếp hoặc qua trò chuyện video để đảm bảo đó là nhân viên chiến dịch hoặc tình nguyện viên thực sự. Chỉ chia sẻ mật khẩu trực tiếp hoặc qua các tin nhắn được mã hóa trong thời gian ngắn. Không bao giờ chia sẻ mật khẩu qua email hoặc lưu trữ/phân phối bằng hệ thống bộ phận trợ giúp.

3. **Sử dụng các trình quản lý mật khẩu** như LastPass, 1Password hoặc Dashlane để giúp bạn quản lý nhiều mật khẩu dài, mạnh một cách dễ dàng. Nhưng hãy đảm bảo rằng hệ thống quản lý của bạn có mật khẩu dài, mạnh và xác thực hai yếu tố. Chúng tôi hiện không khuyến nghị các trình quản lý mật khẩu được tích hợp trong trình duyệt, thường kém an toàn hơn các trình quản lý độc lập này.

TRÌNH QUẢN LÝ MẬT KHẨU

Trình quản lý mật khẩu là một cách để lưu trữ, truy xuất và tạo mật khẩu. Một số thậm chí còn có khả năng tự động điền dòng mật khẩu trên các trang đăng nhập. Trình quản lý mật khẩu yêu cầu mật khẩu riêng để đăng nhập, mật khẩu này trở thành mật khẩu duy nhất bạn phải nhớ. Tất nhiên, rủi ro là nếu ai đó đột nhập vào trình quản lý mật khẩu của bạn (điều đó đã xảy ra), người đó sẽ có tất cả mật khẩu của bạn. Nhưng rủi ro này hầu như luôn vượt xa lợi ích của mật khẩu mạnh, duy nhất trên tất cả các tài khoản của bạn. Đối với các chiến dịch, trình quản lý mật khẩu đôi khi có ý nghĩa đối với các tài khoản có nhiều người dùng, vì quản trị viên có thể chia sẻ quyền truy cập vào họ một cách an toàn.

4. **Tạo tài khoản riêng cho quản trị viên và người dùng**, đồng thời hạn chế nghiêm ngặt quyền truy cập vào tài khoản quản trị viên. Quản trị viên cũng nên có hai tài khoản chiến dịch riêng biệt—một tài khoản chỉ được sử dụng cho nhiệm vụ quản trị của họ và một tài khoản là tài khoản người dùng tiêu chuẩn của họ cho tất cả các hoạt động kinh doanh chiến dịch khác. Điều này sẽ làm giảm khả năng kẻ thù có thể xâm phạm tài khoản quản trị viên, tài khoản này sẽ cung cấp quyền truy cập vào toàn bộ mạng.

5. Tiến hành **đánh giá định kỳ** về những người có quyền truy cập vào các thiết bị và mạng khác nhau. Chặn ngay quyền truy cập của những người rời khỏi chiến dịch. Thay đổi mật khẩu ngay lập tức nếu quan sát thấy hoạt động đáng ngờ.

QUẢN TRỊ VIÊN

Trong "nói về CNTT", "quản trị viên" hoặc "quản trị viên" có khả năng cấp cho mọi người quyền truy cập hoặc kiểm soát vào các hệ thống hoặc thông tin. Ví dụ: với tư cách là "quản trị viên" cho hệ thống email, bạn có thể tạo tài khoản, thay đổi mật khẩu và đặt các yêu cầu như độ dài mật khẩu và xác thực hai yếu tố cho tất cả các tài khoản. Trong bộ ứng dụng văn phòng như GSuite hoặc Microsoft 365, bạn cũng có thể tạo nhóm, chẳng hạn như "Nhóm hiện trường" hoặc "Nhóm truyền thông". Công việc của một quản trị viên thực sự quan trọng. Nếu họ làm đúng, thông tin sẽ chỉ có sẵn cho những người cần nó, điều này rất cần thiết cho bảo mật. Điều này có nghĩa là việc quyết định ai nhận được đặc quyền quản trị viên cũng là một quyết định quan trọng. Chỉ một vài người, rất đáng tin cậy mới có thể

"Nâng cao" - Thực hiện bước tiếp theo

1. **Tạo hồ sơ người dùng cho các loại nhân viên chiến dịch khác nhau** để tự động cấp cấp cấp độ truy cập cần thiết. Các loại nhân viên khác nhau — thực tập sinh, nhân viên hiện trường, lãnh đạo chiến dịch — yêu cầu quyền truy cập vào các nguồn lực khác nhau. Có hồ sơ được xác định trước giúp đảm bảo rằng mọi người chỉ có quyền truy cập vào những gì họ cần.

Bước 4: Lập kế hoạch ứng phó sự cố

Điều quan trọng là lập kế hoạch ứng phó với một cuộc tấn công cũng như phát triển một chiến lược bảo mật để ngăn chặn một cuộc tấn công. Cách bạn phản ứng thường liên quan nhiều đến kết quả cuối cùng của một sự cố hơn là những gì đã bị xâm phạm. Bạn nên dành thời gian cho các khóa tu chiến lược hoặc các cuộc họp nhân viên cấp cao dài hơn để thảo luận về điều gì sẽ xảy ra nếu có điều gì đó xảy ra. Dưới đây là danh sách kiểm tra các bước bạn nên thực hiện:

Hợp pháp:

- **Xác định luật sư bên ngoài** mà bạn sẽ thuê lại trong trường hợp xảy ra sự cố mạng và thảo luận về quy trình ứng phó với họ khi bắt đầu chiến dịch. Trong hầu hết các trường hợp, đây sẽ là cùng một người đại diện cho chiến dịch của bạn về các vấn đề khác, nhưng lý tưởng nhất là bạn sẽ có một người chuyên ứng phó sự cố theo cuộc gọi, chuyên nghiệp hoặc giữ lại 0 đô la.
- Yêu cầu luật sư của bạn giải thích các **nghĩa vụ pháp lý của bạn** nếu dữ liệu bị đánh cắp và những biện pháp tuân thủ nào bạn sẽ cần áp dụng.
- Hiểu nghĩa **vụ pháp lý của nhà cung cấp trong** việc thông báo cho bạn hoặc những người khác nếu họ bị tấn công. Bất cứ khi nào có thể, hãy bao gồm các yêu cầu thông báo nghiêm ngặt trong hợp đồng nhà cung cấp của bạn, vì các bên thứ ba là nguồn vi phạm thường xuyên.
- Nếu bạn tin rằng bạn đã bị vi phạm, cách tốt nhất là luật sư của bạn **giám sát phản ứng của bạn** theo đặc quyền luật sư-khách hàng.
- Nói chuyện với luật sư của bạn về cách tốt nhất để **làm việc với cơ quan thực thi pháp luật** nếu xảy ra vi phạm. Mỗi chiến dịch sẽ tiếp cận điều này khác nhau.

Kỹ thuật:

- Xác định trước bạn **sẽ gọi ai để được hỗ trợ kỹ thuật** nếu bạn nghĩ rằng mình đã bị tấn công. Cuộc họp kín của tiểu bang hoặc ủy ban đảng quốc gia của bạn thường có thể cung cấp giới thiệu.
- Chọn **ai đó trong chiến dịch sẽ giao tiếp với các chuyên gia kỹ thuật** trong trường hợp vi phạm. Lý tưởng nhất là cùng một người đã điều phối CNTT cho chiến

dịch. Quản lý ứng phó sự cố có thể khiến bạn choáng ngợp, vì vậy bạn muốn ai đó tập trung vào các khía cạnh kỹ thuật, người biết họ đang làm gì. Bằng cách đó, bạn có thể tập trung vào việc giao tiếp với các bên liên quan và báo chí.

Hoạt động:

- Quyết định trước **ai sẽ tham gia Nhóm Ứng phó Sự cố** (IRT) của bạn và ai sẽ tham gia các cuộc họp ứng phó sự cố. Điều quan trọng là phải bao gồm một người nào đó từ nhóm CNTT, pháp lý, vận hành và truyền thông của bạn. Nếu bạn là một chiến dịch nhỏ và không có hỗ trợ truyền thông, CNTT hoặc hoạt động toàn thời gian, hãy lên kế hoạch bao gồm bất kỳ nhân viên chủ chốt nào giám sát hoạt động của chiến dịch.

- Xác định chuỗi **chỉ huy để ra quyết định** trong trường hợp vi phạm, đặc biệt là liên quan đến thông tin liên lạc. Trong nhiều trường hợp, đây sẽ là người quản lý chiến dịch, nhưng một số người quản lý có thể chọn ủy thác trách nhiệm cho người khác.

- Xác định **ứng dụng hoặc công nghệ bạn sẽ sử dụng để liên lạc** nếu bạn nghĩ rằng email của mình đã bị vi phạm (Signal và Wickr là hai tùy chọn phổ biến).
  Giao tiếp trong một vụ vi phạm là điều cần thiết, nhưng bạn không muốn đối thủ của mình biết bạn đang nói gì — hoặc thậm chí bạn đang phản ứng với hành động của họ.

Truyền thông:

- **Tiến hành lập kế hoạch kịch bản**. Đối với nhiều chiến dịch, đây có thể là một phần của chiến lược hiện có. Đối với các chiến dịch lớn hơn có rủi ro cao hơn, có thể cần phải có một cuộc họp chuyên dụng. Lập kế hoạch kịch bản của bạn nên bao gồm:

  a. **Xác định các bên liên quan chính bên trong và bên ngoài**, như nhân viên, tình nguyện viên, nhà tài trợ và người ủng hộ của bạn. Biết bạn cần liên hệ với ai nếu có sự cố xảy ra và xếp hạng họ theo thứ tự ưu tiên. Xây dựng danh sách liên hệ và chỉ định ai sẽ liên hệ với họ.

  b. **Động não các tình huống gây thiệt hại nhất** và xem xét các bên liên quan và thông điệp của bạn có thể thay đổi như thế nào đối với từng tình huống.

     Các tình huống khác nhau có thể bao gồm:

     - Tin đồn rằng chiến dịch của bạn đã bị tấn công;
     - Thẻ tín dụng và thông tin liên hệ của các nhà tài trợ của bạn bị đánh cắp;
     - Ransomware và một nỗ lực tống tiền được đưa ra chống lại chiến dịch của bạn;
     - Hệ thống của bạn bị xóa và tắt;
     - Email của ai đó bị đánh cắp;

- Đối thủ của bạn đánh cắp thông tin đăng nhập của quản trị viên và mọi tệp trên ổ đĩa chiến dịch của bạn.

- **Hãy cẩn thận với những gì bạn nói trong hiện tại về chính sách an ninh mạng** hoặc các sự cố mạng. Một số nạn nhân của tội phạm mạng trước đây đã đưa ra những tuyên bố hoành tráng về các biện pháp an ninh của chính họ, hoặc đã chỉ trích những người khác đã bị tấn công. Báo chí sẽ buộc bạn phải chịu trách nhiệm về những gì bạn đã nói trong quá khứ nếu bạn trở thành nạn nhân.

- Tương tự, tránh **cung cấp thông tin chi tiết về phạm vi của sự kiện trong giai đoạn đầu của** sự cố (và nếu bạn có thể tránh thảo luận hoàn toàn về phạm vi, thậm chí còn tốt hơn). Thông tin chi tiết có sẵn ngay từ đầu sẽ thay đổi khi bạn điều tra. Một sai lầm phổ biến là nói điều gì đó mà sau đó hóa ra không đúng sự thật (ví dụ: "họ không ăn cắp nhiều" hoặc "không có thông tin cá nhân nào bị lấy đi"). Chỉ nói những gì bạn biết *chắc chắn* là cách an toàn nhất. Các tuyên bố nên tập trung vào các hành động bạn đang thực hiện để làm cho tình hình phù hợp với các bên liên quan bị ảnh hưởng.

- **Phát triển trước một số ngôn ngữ nguyên mẫu** để bạn có thể soạn thảo các tuyên bố hoặc quan điểm nói chuyện một cách nhanh chóng nếu có sự cố xảy ra. Tối thiểu, hãy tạo một tài liệu hỏi đáp đơn giản mà bạn có thể nhanh chóng sửa đổi nếu bạn thực sự cần sử dụng nó. Tạo tài liệu hỏi đáp trước sẽ giúp bạn suy nghĩ nhiều về những gì bạn *sẽ không* nói cũng như những gì bạn *sẽ nói* . Ví dụ, câu hỏi đầu tiên thường là, "Chuyện gì đã xảy ra?" Tuy nhiên, bạn có thể không trả lời được điều đó trong nhiều ngày hoặc vài tuần. Thực tế là bạn không biết loại vi phạm nào sẽ xảy ra thực sự có thể giúp bạn viết trước các câu trả lời soạn mẫu tốt hơn.

  Các câu hỏi cần đưa vào tài liệu hỏi đáp của bạn là:

  - Điều gì đã xảy ra?
  - Làm thế nào nó xảy ra?
  - Ai đã làm điều đó?
  - Những gì đã bị đánh cắp hoặc hư hỏng?
  - Thông tin cá nhân của ai đó có bị đánh cắp không? Bạn đang làm gì để bảo vệ họ?
  - Các tin tặc đã làm điều đó như thế nào?
  - Tin tặc có ra khỏi hệ thống của bạn không?
  - Họ đã ở trong hệ thống của bạn bao lâu?
  - Bạn đã có những biện pháp bảo mật nào? Tại sao chúng không hiệu quả?
  - Bạn không nên biết điều này sẽ xảy ra sao? Tại sao hệ thống của bạn không được bảo mật tốt hơn?
  - Bạn có đang làm việc với cơ quan thực thi pháp luật không? Cơ quan thực thi pháp luật đã liên hệ với bạn chưa?

- Trong một vụ vi phạm ransomware, bạn sẽ được hỏi: Bạn đã trả tiền chuộc và tại sao hoặc tại sao không?

- **Giữ liên lạc với các bên liên quan chính của bạn và** cập nhật thông tin cho họ nhất có thể. Bạn có thể sẽ không thể nói nhiều, nhưng liên hệ với họ thường xuyên với những gì bạn biết, có tuyên bố rõ ràng về ý định của bạn và cung cấp thông tin chi tiết về những gì bạn đang làm để quản lý tình huống là chìa khóa. Tránh đặt
  kỳ vọng về các bản cập nhật quá thường xuyên, bởi vì thường thì bạn sẽ không có thông tin mới và các bên liên quan của bạn sẽ trở nên thất vọng nếu bạn tiếp tục quay lại với họ mà không có thông tin mới. Chỉ chủ động nói chuyện với giới truyền thông nếu bạn có thông tin mới để cung cấp.

Bước 5: Thiết bị

Mọi thiết bị vật lý trong chiến dịch của bạn—từ điện thoại di động, máy tính bảng hoặc máy tính xách tay đến bộ định tuyến, máy in hoặc máy ảnh—đại diện cho một đường tấn công tiềm ẩn vào mạng của bạn. Một kế hoạch an ninh mạng tốt sẽ cố gắng kiểm soát quyền truy cập vào, vào và trên *tất cả các* thiết bị. Bạn có thể kiểm soát quyền truy cập *vào* các thiết bị bằng cách đảm bảo chúng luôn được xử lý và tính toán đúng cách. Bạn kiểm soát quyền truy cập *vào* các thiết bị thông qua xác thực hai yếu tố và mật khẩu mạnh. Bạn kiểm soát nội dung *trên* thiết bị thông qua mã hóa và các chính sách hướng dẫn cách bạn lưu trữ dữ liệu (tức là lưu trữ thông tin trên đám mây thay vì trên máy).

"Tốt" - Những gì bạn cần làm

1. **Luôn sử dụng hệ điều hành (HĐH) cập nhật nhất** hiện có, vì các bản cập nhật hệ thống thường bao gồm các bản vá cho các lỗ hổng mới nhất. Nếu có thể, hãy đặt cài đặt thiết bị để **tự động cài đặt các** bản cập nhật này. Hãy làm cho công việc của ai đó là kiểm tra thường xuyên xem mọi người đều cập nhật.
2. **Sử dụng dịch vụ sao lưu tự động dựa trên đám mây** để giảm thiểu tác động của mất dữ liệu nếu thiết bị bị mất hoặc bị đánh cắp. Ví dụ bao gồm Backblaze và CrashPlan.
3. **Quyền truy cập vật lý vào thiết bị**
   a. Ngay từ đầu, lãnh đạo chiến dịch nên **tạo ra một môi trường** trong đó mọi người coi trọng bảo mật vật lý của thiết bị của họ - việc mất thiết bị có thể cho phép đối thủ truy cập vào thông tin quan trọng có thể được sử dụng để làm tổn hại đến chiến dịch.

b. Mặc dù nhiều chiến dịch không đủ khả năng mua thiết bị mới, nhưng tốt nhất bạn nên **mua thiết bị mới (đặc biệt là máy tính và điện thoại) nếu có thể.** Tối thiểu, bạn nên cung cấp thiết bị mới cho nhân viên làm việc với dữ liệu nhạy cảm.

c. Nếu nhân viên đang sử dụng máy tính và điện thoại của riêng họ, hãy **thiết lập chính sách "Mang thiết bị của riêng bạn" (BYOD)** thực hiện các biện pháp bảo mật mạnh mẽ (xem bảo vệ điểm cuối bên dưới).

d. **Các thành viên chiến dịch KHÔNG nên sử dụng tài khoản email cá nhân hoặc thiết bị không được bảo mật theo chính sách BYOD** cho hoạt động kinh doanh của chiến dịch, bao gồm cả email và phương tiện truyền thông xã hội. Bất kỳ thông tin quan trọng nào nằm bên ngoài các thiết bị hoặc hệ thống do chiến dịch kiểm soát đều dễ bị tấn công. Lãnh đạo nên liên tục củng cố rằng dữ liệu chiến dịch cần phải tránh xa email cá nhân và máy tính không an toàn.

e. **Báo cáo thiết bị bị mất ngay lập tức**. Yêu cầu cài đặt mặc định cho phép **xóa từ xa** trên tất cả các thiết bị.

f. Thắng hay thua, hãy **có kế hoạch cho những gì xảy ra với tất cả dữ liệu, tài khoản** và thiết bị khi chiến dịch kết thúc. Hậu quả ngay sau một chiến dịch là một giai đoạn đặc biệt dễ bị tổn thương.

4. Truy cập kỹ thuật số vào các thiết bị

a. Thay đổi **mật khẩu và cài đặt mặc định** trên tất cả các thiết bị. Nhiều thiết bị xuất xưởng với mật khẩu mặc định thực sự dễ đoán. Ngoài ra, hãy tắt tài khoản khách nếu thiết bị đi kèm.

b. Thực hiện **tự động khóa** cho điện thoại và máy tính sau hai phút và yêu cầu **mật khẩu** hoặc ID vân tay để mở khóa.

5. Nội dung trên thiết bị

a. Yêu cầu **mã hóa** trên tất cả các thiết bị (máy tính và điện thoại) để đảm bảo rằng việc mất thiết bị không có nghĩa là nội dung của nó bị xâm phạm. Ví dụ bao gồm FileVault cho Mac và BitLocker cho Windows. Một số thiết bị như iPhone thực hiện điều này theo mặc định, nhưng không phải tất cả đều làm được.

b. Cài đặt **phần mềm bảo vệ điểm cuối** trên tất cả các thiết bị. Một số ví dụ bao gồm Trend Micro, Sophos và Windows Defender. Có các ứng dụng bảo mật điểm cuối đặc biệt cho điện thoại và máy tính bảng. Lookout là một ví dụ.

BẢO VỆ ĐIỂM CUỐI LÀ GÌ?

Điểm cuối là các thiết bị mà nhân viên sử dụng, bao gồm điện thoại di động, máy tính xách tay và máy tính để bàn. Họ là "điểm cuối" của mạng lưới chiến dịch và nhân viên là "người dùng cuối". Bảo vệ điểm cuối kiểm soát tập trung và quản lý bảo mật trên các thiết bị từ xa. Điều này đặc biệt quan trọng đối với các chiến dịch cho phép nhân viên "mang theo thiết bị của riêng bạn" (BYOD), vì chiến dịch cần đảm bảo rằng thiết bị an toàn, không có phần mềm độc hại và có thể bị xóa nếu bị đánh cắp hoặc bị mất. Bảo vệ điểm cuối cũng có thể giám sát thiết bị để đảm bảo phần mềm được cập nhật và phát hiện phần mềm độc hại mới hoặc các mối đe dọa tiềm ẩn. Đối với nhiều chiến dịch, điều này sẽ giống như một sự nâng đỡ lớn, nhưng xây dựng nó vào thói quen giới thiệu của bạn và đầu tư

"Nâng cao" - Thực hiện bước tiếp theo

1. **Sử dụng phần mềm quản lý thiết bị di động (MDM)** để giám sát hoạt động để đảm bảo tất cả các thiết bị tuân thủ các chính sách bảo mật điện thoại di động và thiết bị người dùng mà bạn đã thiết lập cho chiến dịch của mình. Ví dụ bao gồm VMware AirWatch, Microsoft InTune và JAMF. GSuite và Microsoft Office 365 cũng bao gồm một dịch vụ MDM.

2. **Sử dụng các dịch vụ bảo vệ mối đe dọa nâng cao** để giám sát và cảnh báo hoạt động độc hại, chẳng hạn như CrowdStrike Falcon hoặc Mandiant FireEye. Crowdstrike đôi khi cung cấp dịch vụ ngăn chặn vi phạm Falcon miễn phí thông qua Crowdstrike Foundation, tùy thuộc vào nhu cầu của chiến dịch và các quy tắc tài chính chiến dịch của bạn.

Bước 6: Mạng

Mạng là hệ thống phần cứng vật lý, phần mềm kỹ thuật số và các kết nối của chúng. Chúng đại diện cho một môi trường tấn công giàu mục tiêu khác. Bảo mật mạng bao gồm mọi thứ, từ cách các thiết bị giao tiếp với nhau đến sử dụng các dịch vụ đám mây để lưu trữ dữ liệu.

"Tốt" - Những gì bạn cần làm

1. **Nắm bắt đám mây.** Lưu trữ dữ liệu trên các dịch vụ đám mây, không phải trên máy tính cá nhân hoặc máy chủ. Bất cứ thứ gì được lưu trữ trên thiết bị cá nhân đều phải đối mặt với rủi ro cao hơn đám mây.
    a. Không ai có quyền truy cập vào tất cả các tệp trên mạng; Không nên sử dụng tài khoản có quyền truy cập quản trị viên toàn diện cho công việc hàng ngày. Chia bộ nhớ tệp của bạn thành các thư mục của bộ phận và cấp quyền truy cập cho phù hợp.
    b. Đảm bảo quyền truy cập vào nội dung được chia sẻ chỉ bằng lời **mời**. Một số dịch vụ quản lý tệp cũng cho phép thực hiện ngày hết hạn đối với lời mời và quyền truy cập.
    c. Kiểm tra định kỳ những gì đang được chia sẻ và với ai.
2. **Có một mạng wifi "khách" riêng cho** khách truy cập và tình nguyện viên hạn chế quyền truy cập của họ vào các tài nguyên chiến dịch. Cố gắng mua các bộ định tuyến cung cấp "hồ sơ khách" sẽ tự động phân đoạn mạng của bạn.
3. Khi đi du lịch hoặc trước khi bạn thiết lập văn phòng chiến dịch của mình, **hãy tránh các dịch vụ wifi công cộng càng nhiều càng tốt** và sử dụng mạng wifi đáng tin cậy bất cứ khi nào có thể. Nếu bạn cần wifi di động, hãy cố gắng cung cấp cho nhân viên chiến dịch các điểm truy cập wifi di động để chia sẻ kết nối. Wifi công cộng thường miễn phí và dễ kết nối, nhưng những kẻ tấn công cũng có thể sử dụng nó để xâm nhập vào phần cứng của bạn.
    a. Nếu có thể, nhân viên nên **sử dụng VPN** (mạng riêng ảo). VPN giúp bảo vệ chống lại những kẻ xâm nhập khi sử dụng wifi công cộng. Ví dụ về dịch vụ VPN bao gồm ExpressVPN hoặc TunnelBear. Không phải tất cả các VPN đều được tạo ra như nhau. Hãy cẩn thận với các dịch vụ miễn phí: nhiều người đang tìm cách lấy dữ liệu của bạn!
4. **Bảo mật trình duyệt của bạn.** *Tạp chíPC* xếp hạng Chrome và Firefox là hai trình duyệt an toàn nhất vào năm 2017. Bất kể bạn sử dụng trình duyệt nào, hãy cập nhật trình duyệt.

VPN

Mạng riêng ảo (VPN) là một "đường hầm" được mã hóa cho lưu lượng truy cập Internet của bạn, che giấu nó khỏi những kẻ xâm nhập. Một số văn phòng sử dụng nó như một cách để đăng nhập từ xa vào mạng văn phòng, nhưng điều này không phổ biến lắm đối với các chiến dịch. Các chiến dịch nên xem xét việc nhân viên của họ sử dụng VPN trên máy tính và điện thoại di động nếu họ thường xuyên phải sử dụng wifi công cộng hoặc mạng không đáng tin cậy (đôi

"Nâng cao" - Thực hiện bước tiếp theo

1. Bạn có thể thực hiện các bước nâng cao hơn để bảo vệ mạng của mình, nhưng chúng nên được **thực hiện bởi một chuyên gia CNTT**. Chúng tôi khuyên bạn nên yêu cầu họ bao gồm những điều sau:

    a. **Thiết lập tường lửa phần cứng**.

    b. **Mã hóa kết nối wifi của bạn** bằng các giao thức bảo mật WPA2 hoặc 802.1x (không sử dụng WEP).

    c. Định cấu hình proxy web dựa trên đám mây để **chặn quyền truy cập vào các trang web đáng ngờ** từ bất kỳ thiết bị nào thuộc sở hữu của chiến dịch, bất kể nó ở đâu. Ví dụ về nhà cung cấp dịch vụ bao gồm Zscaler, Cisco Umbrella và Dịch vụ đám mây McAfee Web Gateway.

    d. Lưu trữ nhật ký hoạt động của bạn trên nhà cung cấp dịch vụ đám mây như LogEntries hoặc SumoLogic.

    e. **Phân đoạn bộ nhớ dựa trên đám mây của bạn** để không phải mọi thứ được lưu trữ ở cùng một nơi. Nghiên cứu của phe đối lập, bản ghi nhớ chiến lược và hồ sơ nhân sự nên được giữ trong các thư mục khác nhau và quyền truy cập vào các thư mục đó nên được hạn chế cho những người thực sự cần chúng. Hãy xem xét một hệ thống lưu trữ hoàn toàn khác cho thông tin nhạy cảm nhất của chiến dịch của bạn. Hạn chế quyền truy cập để chỉ những nhân viên chủ chốt mới có thể truy cập và chỉ khi sử dụng các thiết bị cụ thể. (Ví dụ: nếu bạn sử dụng Microsoft365 cho bộ ứng dụng văn phòng và lưu trữ tài liệu, nhưng tài liệu nhạy cảm nhất của bạn trên tài khoản Dropbox hoặc Box.) Nếu một thành viên của chiến dịch bị xâm phạm, kiểu phân khúc này có thể hạn chế thiệt hại.

2. **Đào tạo nhân viên không kết nối thiết bị của họ với các cổng hoặc thiết bị không xác định**. Không sử dụng bộ sạc công cộng tại sân bay hoặc sự kiện. Không chấp nhận bộ sạc điện thoại hoặc pin miễn phí tại các sự kiện (ổ USB miễn phí đó có thể chứa phần mềm độc hại!).

Bạn có thấy cách để làm cho Playbook này tốt hơn không?

Có công nghệ hoặc lỗ hổng mới nào mà chúng ta nên giải quyết không?

Chúng tôi muốn phản hồi của bạn.

Vui lòng chia sẻ ý tưởng, câu chuyện và nhận xét của bạn trên Twitter @d3p sử dụng hashtag #CyberPlaybook hoặc gửi email cho chúng tôi theo địa chỉ connect@d3p.org để chúng tôi có thể tiếp tục cải thiện tài nguyên này khi môi trường kỹ thuật số thay đổi.

Dự án Bảo vệ Dân chủ Kỹ thuật số
Trung tâm Khoa học và Các vấn đề Quốc tế
Belfer Trường Harvard Kennedy
79 Phố John F. Kennedy Cambridge,
MA 02138

www.belfercenter.org/D3P