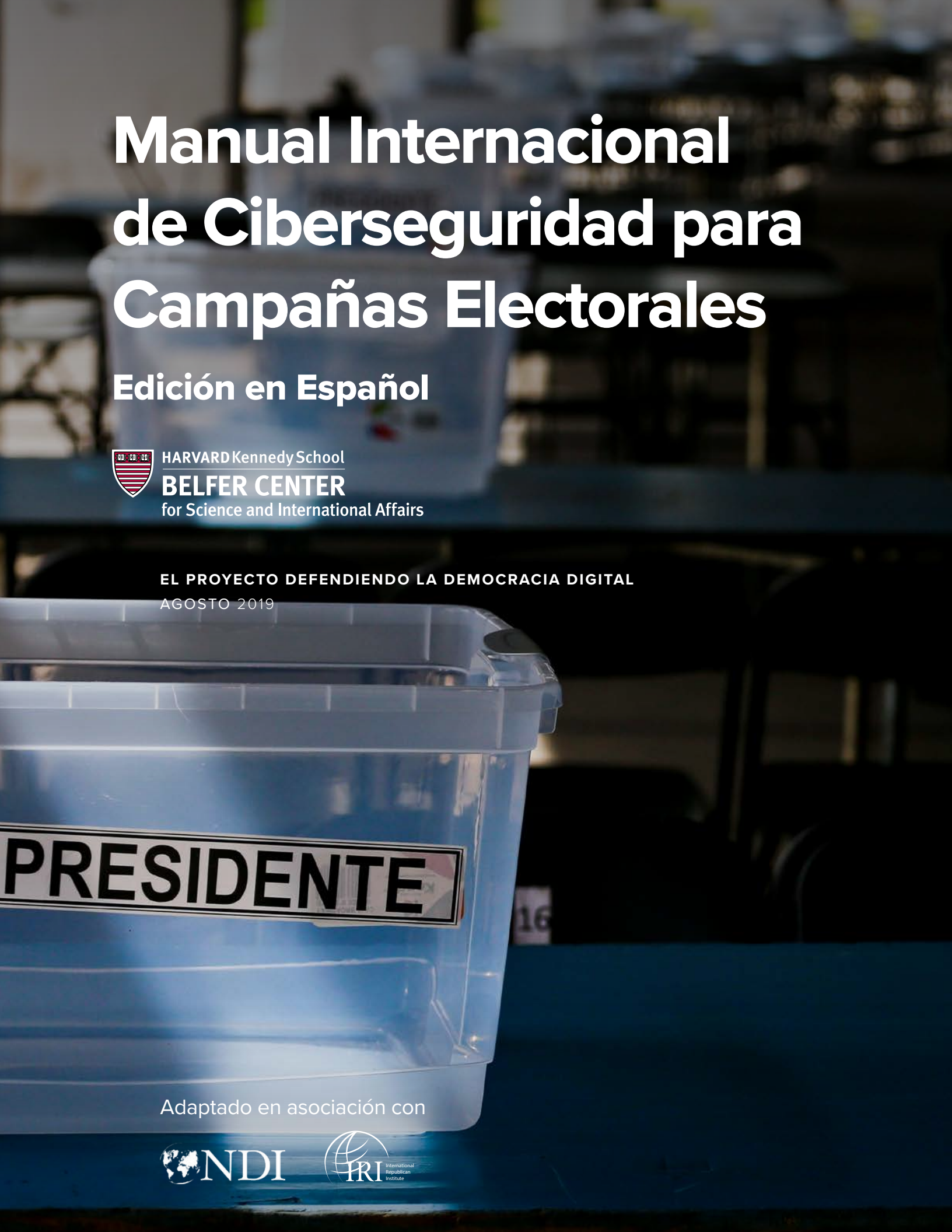
Manual Internacional de Ciberseguridad para Campañas Electorales

Edición en Español

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

EL PROYECTO DEFENDIENDO LA DEMOCRACIA DIGITAL

AGOSTO 2019



Adaptado en asociación con

NDI

IRI International Republican Institute

El Proyecto Defendiendo la Democracia Digital
Centro de Ciencias y Asuntos Internacionales Belfer
Facultad Kennedy de Harvard
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Socios de la edición en español:

The National Democratic Institute
www.ndi.org

The International Republican Institute
www.iri.org

Agradecemos especialmente al Programa de Protección de Elecciones Democráticas de Microsoft, por su apoyo en la edición del manual en español.

Diseño por Andrew Facini.

Foto de cubierta: Una línea de las urnas que dice: "Presidente" colocado en preparación para la segunda vuelta presidencial dentro del Estadio Nacional utilizado como centro de votación en Santiago, Chile, el sábado 16 de diciembre de 2017.

Translation in progress | Working draft 2019-08-26

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

EL PROYECTO DEFENDIENDO LA DEMOCRACIA DIGITAL
AGOSTO 2019

Manual de Ciberseguridad para Campañas Electorales

Edición en Español

Contenido

Bienvenido

Las personas se unen a una campaña por distintas razones: elegir a un líder al cual le tienen confianza, promover una agenda, mejorar el gobierno o experimentar la fuerza y la adrenalina de la vida en campaña. Estas son algunas de las razones por las cuales nos involucramos en la política. Pero ciertamente no nos apuntamos porque queríamos ser cíberexpertos y suponemos que usted tampoco.

Desafortunadamente, las amenazas a la seguridad están creciendo y cuentan con el potencial para afectar su campaña íntegramente. Venimos de un mundo de campañas y de apoyar procesos democráticos internacionales y hemos visto de primera mano las formas en que los piratas informáticos, la desinformación y la captura de páginas web pueden afectar el curso de una elección, así como la dirección de un país.

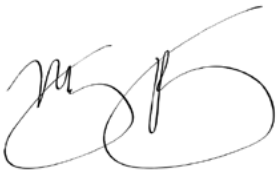
D3P es un equipo bipartidario de expertos en ciberseguridad y políticas provenientes de los sectores público y privado, así como expertos con profunda experiencia en campañas políticas. Nos hemos asociado con el Instituto Republicano Internacional (IRI) y el Instituto Nacional Demócratico (NDI) para comprender mejor el panorama de las elecciones internacionales y cómo reflexionar acerca de los riesgos digitales y protegernos de ellos.

Formamos parte de distintos partidos políticos y no coincidimos en muchas aspectos cuando se trata de políticas públicas, pero lo que sí nos une es la convicción de que son solamente los votantes quienes debieran decidir nuestras elecciones. Nuestras formas de vivir y trabajar cada vez más digitales abren nuevas vías para que los adversarios influyan sobre nuestras campañas y elecciones. Si bien no tienes que ser un ciberexperto para dirigir una campaña exitosa, sí tienes la responsabilidad de proteger a tu candidato y organización de los adversarios en el espacio digital. Fue por dicha razón que "Defensa de la democracia digital" (*Defending Digital Democracy*), un proyecto del Centro de Ciencias y Asuntos Internacionales Belfer (*Belfer Center for Science and International Affairs*) de la facultad Kennedy de Harvard (*Harvard Kennedy School*) creó este Manual de campaña de ciberseguridad (**Cybersecurity Campaign Playbook** [PDF]). El Instituto Nacional Demócrata para los Asuntos Internacionales, el Instituto Republicano Internacional y decenas de funcionarios electos, expertos en seguridad y profesionales en campañas trabajaron en el proyecto "Defensa de la democracia digital", para así adaptar este manual a un contexto internacional más amplio.

La información aquí recopilada es para todo tipo de campaña y para cualquier partido. Está diseñada para brindarle información simple con la cual actuar, y procurar que la información de su campaña esté más segura frente a los adversarios que intenten atacar su organización y la democracia de su país. Esperamos sobre todo que este recurso le permita pasar más tiempo haciendo aquello para lo cual realmente se involucro: hacer campaña.

Buena suerte.

Robby Mook
Director de campaña de Hillary Clinton 2016.



Matt Rhoades
Director de campaña de Mitt Romney 2012.

P.D. ¿Piensa usted en algunas formas de mejorar este manual? ¿Conoce nuevas tecnologías o vulnerabilidades a las que debiéramos responder? Queremos recibir sus sugerencias. Por favor comparta sus ideas, historias y comentarios en Twitter @d3p con el hashtag #CyberPlaybook, o escríbanos a connect@d3p.org para que así podamos seguir mejorando este herramineta a medida que el entorno digital vaya cambiando.

Autores y colaboradores

Este proyecto fue posible gracias a decenas de personas que generosamente aportaron su tiempo de forma voluntaria. Un especial agradecimiento al grupo de revisores voluntarios que aconsejaron la adaptación de la edición en español del manual. Agradecemos especialmente a **Debora Plunkett** por liderar el proyecto y a **Harrison Monsky** por redactar el documento. También agradecemos a las personas que listamos abajo, quienes dedicaron mucho tiempo a revisar borradores y aportar sugerencias.

Agradecemos especialmente al Programa de Protección de Elecciones Democráticas de Microsoft, por su apoyo en la edición del manual en español.

DEFENSA DE LA DEMOCRACIA DIGITAL LÍDERES

Eric Rosenbach, Co-Director, Belfer Center

María Barsallo Lynch, Executive Director

Robby Mook, Belfer Center Senior Fellow

Matt Rhoades, D3P Senior Advisor

AUTORES Y COLABORADORES

Heather Adkins, Director, Information Security and Privacy, Google

Dmitri Alperovitch, Co-founder and CTO, CrowdStrike

Ryan Borkenhagen, IT Director, Democratic Senatorial Campaign Committee

Josh Burek, Director of Global Communications and Strategy, Belfer Center

Michael Chenderlin, Chief Digital Officer, Definers Public Affairs

Robert Cohen, Cyber Threat Analyst, K2 Intelligence

Chris Collins, Co-Founder, First Atlantic Capital

Caitlin Conley, D3P, Harvard Kennedy School

Julia Cotrone, Special Assistant, Definers Public Affairs

Jordan D'Amato, D3P, Harvard Kennedy School

Mari Dugas, Project Coordinator, D3P, Harvard Kennedy School

Josh Feinblum, D3P, Massachusetts Institute of Technology

John Flynn, Chief Information Security Officer, Uber

Siobhan Gorman, Director, Brunswick Group

Daniel Griggs, Founder and CEO, cmdSecurity Inc.

Stuart Holliday, CEO, Meridian International Center

Eben Kaplan, Principal Consultant, CrowdStrike

Greg Kesner, Principal, GDK Consulting

Kent Lucken, Managing Director, Citibank

Katherine Mansted, D3P, Harvard Kennedy School

Ryan McGeehan, Member, R10N Security

Jude Meche, Chief Technology Officer, Democratic Senatorial Campaign Committee

Nicco Mele, Director, Shorenstein Center

Eric Metzger, Founding Partner and Managing Director, cmdSecurity Inc.

Zac Moffatt, CEO, Targeted Victory

Harrison Monsky, D3P, Harvard Law School

Debora Plunkett, Former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Jim Routh, Chief Security Officer, Aetna

Suzanne E. Spaulding, Senior Adviser for Homeland Security, Center for Strategic and International Studies

Matthew Spector, D3P, Harvard Kennedy School

Irene Solaiman, D3P, Harvard Kennedy School

Jeff Stambolsky, Security Response Analyst, CrowdStrike

Alex Stamos, Chief Security Officer, Facebook

Phil Venables, Partner and Chief Operational Risk Officer, Goldman Sachs

Frank White, Independent Communications Consultant

Sally White, D3P, Harvard University

Rob Witoff, Senior Security Manager, Google

Contributors from the **National Democratic Institute** and the **International Republican Institute**

CENTRO BELFER DISEÑADOR

Andrew Facini, Publishing Manager

El enfoque del manual

Este manual internacional de ciberseguridad de campaña fue preparado por un equipo multipartidario e internacional de expertos en ciberseguridad, política y leyes para así brindar formas simples y factibles con que contrarrestar las crecientes ciberamenazas.

Los ciberadversarios no discriminan. Las campañas han sido hackeadas a todo nivel, no solo las internacionales de alto nivel. Usted deberá asumir que es un blanco. Si bien las recomendaciones de este manual son universalmente aplicables, están dirigidas fundamentalmente a aquellas campañas que no cuentan con los recursos necesarios para contratar personal profesional de ciberseguridad. Ofrecemos las piezas básicas de una estrategia de ciberseguridad de mitigación de riesgos para que puedan implementarla personas sin preparación técnica (pero sí incluimos algunas areas que requerirán de la ayuda de profesionales de las tecnologías de la información (TI)).

Estas recomendaciones son un punto de partida y no una presentación exhaustiva con la cual alcanzar el nivel más alto posible de seguridad. Alentamos a todas las campañas a que, en la medida que les sea posible, obtengan el apoyo profesional de expertos oficialmente certificados en TI y ciberseguridad.

Introducción

Los candidatos y las campañas enfrentan una gama abrumadora de retos. Hay eventos que organizar, voluntarios a los que reclutar, concentraciones públicas que manejar, fondos que reunir, votantes a los que contactar y las demandas implacables del moderno ciclo mediático. Todo el personal debe prever sorpresas desafortunadas como errores imprevistos o un ataque publicitario de último minuto. Los ciberataques, las campañas de desinformación y la censura en Internet ahora también forman parte de esta lista.

A medida que las campañas se han digitalizado en mayor escala, los adversarios han encontrados nuevas oportunidades para entrometerse, perturbar y robar. En 2008 'hackers' de China se infiltraron en las campañas de Obama y McCain, y robaron gran cantidad de información de ambos. En 2016, las redes sociales de Uganda fueron cerradas durante las elecciones. En 2016, ciberoperativos que se cree fueron auspiciados por el gobierno ruso hurtaron y filtraron decenas de correos electrónicos y documentos del personal de campaña del Partido Demócrata de EE.UU., con lo que alimentaron campañas de información perturbadora. En 2017, los partidos políticos de Kenia enfrentaron extensas campañas de desinformación, y la página web de uno de los principales partidos políticos serbios en Facebook fue eliminada.

Las consecuencias de una ciberviolación de seguridad pueden ser sustanciales. La noticia misma de una falla de seguridad, agravada por la lenta filtración de la información robada, podría sacar de enfoque el mensaje de un candidato durante meses. Si los atacantes sobrecargan una página web pueden cortar la comunicación con sus partidarios o hacer que se pierdan donaciones en momentos claves. El robo de los datos personales de los donantes o votantes podría generar una significativa responsabilidad legal, exponer a los partidarios al acoso y hacer que los donantes duden en contribuir a una campaña. Los ataques destructivos dirigidos a las computadoras personales o a los cruciales servidores de campaña podrían desacelerar las operaciones de campaña durante días o hasta semanas. Resolver los problemas resultantes desviaría recursos preciosos en medio de una carrera reñida, ya sea para presidente o cargos en el congreso o la municipalidad.

Las ciberamenazas seguirán formando parte de nuestro proceso de campaña en el futuro previsible. Al estar a la vanguardia de la democracia, el personal de campaña debe identificar el riesgo de un ataque, diseñar una una estrategia para reducirlo de la mejor manera posible lo más posible e implementar estrategias de respuesta para el momento en que lo peor suceda. Si bien ninguna

campaña puede alcanzar una seguridad perfecta, pero puede tomar unas simples medidas podría hacer que le resulte mucho más difícil a los actores maliciosos hacer daño. Irónicamente, los actores de estado nación más sofisticados frecuentemente eligen los métodos de ataque menos sofisticados, con los que acosan a las personas y organizaciones que descuidan los protocolos de seguridad básicos. Esa es nuestra principal razón para crear esta versión Internacional del Manual de campaña de ciberseguridad.

En las campañas actuales, la ciberseguridad es responsabilidad de todos. Los errores humanos consistentemente han sido la causa principal de los ciberataques conocidos, y le corresponde al candidato y a los dirigentes de la campaña incorporar una concientización de seguridad en la cultura de la organización. Las decisiones que las personas toman son tan importantes como el software que usan. En adelante las mejores campañas tendrán estándares claros de trabajo arduo, concentración en el mensaje, lealtad con el equipo... y la implementación de un protocolo de seguridad.

Planteemos rápidamente el problema antes de pasar a nuestras recomendaciones:

- **el entorno en el cual opera su campaña;**
- **las amenazas que su campaña probablemente enfrentará; y**
- **la importancia de gestionar los ciberriesgos.**

El vulnerable entorno de campaña

Hoy en día, las campañas actuales son blancos excepcionalmente fáciles. A menudo son inherentemente temporales y efímeras. No cuentan con el tiempo ni el dinero para diseñar estrategias de seguridad a largo plazo rigurosamente evaluadas. Un gran número de personal nuevo puede incorporarse rápidamente y sin mucho tiempo de capacitación. Estos pueden traer consigo su propio hardware de casa, junto con el malware alojado en este. Muchos de los que contribuyen a una campaña viven y trabajan a cientos de kilómetros de la oficina central. Los acontecimientos suceden rápidamente, lo que está en juego frecuentemente es muy grande y la gente siente que no tiene tiempo para preocuparse por la ciberseguridad. Hay muchas oportunidades para que algo salga mal.

Al mismo tiempo, las campañas dependen cada vez más de información confidencial acerca de los votantes, los donantes y la opinión pública. También guardan documentación delicada, como investigaciones sobre la oposición, estudios de vulnerabilidad, listas de partidarios, documentos de selección de personal, los primeros borradores de documentos de políticas y correos electrónicos. El riesgo de un posible ataque está creciendo, al igual que las consecuencias.

EL PELIGRO DE UN ATAQUE

Imagina esto: falta un mes para el día de la votación y la carrera está reñida. Llegas temprano a la sede de campaña, te sirves algo de café o té e ingresas a tu computadora. Aparece una pantalla negra, seguida por una espantosa caricatura de tu candidato y un mensaje. Tus discos duros han sido borrados. Toda la información digital que reuniste (memos, listas de focalización, hojas de balance) no está. Lees que recuperarla te costará un millón, o la renuncia a un importante cargo político.

Un grupo no identificado hackeó tu computadora hace meses y ha estado sigilosamente robando correos electrónicos, memos de estrategia, direcciones de los donantes y los números del seguro social y de identidad personal. El grupo se ha pasado semanas revisando el botín en busca de trapos sucios y ha estado distribuyendo lo más destacado en las redes sociales y a través de una página web fácil de usar, dedicada únicamente a esto. En ella figura prominentemente un extenso libro de “autoinvestigación” (self research book) sobre tu candidato. La página web de la campaña no funciona por el momento, sus cuentas en las redes sociales han sido suspendidas por publicar imágenes indecentes y no hay una sola computadora a la vista que funcione.

Las amenazas que las campañas enfrentan

Desafortunadamente para las campañas y las democracias de todo el mundo, los adversarios locales y extranjeros podrían creer que dañar o ayudar a un candidato en particular promueve sus intereses, ya sea que esto quiera decir crear caos y confusión entre los votantes, o castigar a un funcionario que les ha criticado. Esto podría sonar como una novela de suspenso, pero la realidad es que un sofisticado servicio de inteligencia, un cibercriminal o un hacktivista que guarda rencor a un candidato podría decidir que usted o alguien de su campaña es un blanco. Estos son los tipos de amenazas posibles de los que los directores y el personal deben ser conscientes.

A medida que la desinformación y las campañas de comunicaciones manipuladas se convierten en medios para engañar y confundir a los ciudadanos del mundo, la información robada, manipulada y filtrada podría tener consecuencias reales en sus comicios. Los mecanismos con los que cuenta para proteger sus datos y mantener abiertos los canales de comunicación son más importantes que nunca.

¿QUIÉNES SON LOS 'HACKERS'?

Las campañas enfrentan amenazas de información y ciberseguridad provenientes de una amplia gama de actores. Los hackers de "sombrero negro" y los cibercriminales han intentado comprometer campañas por razones de ganancia personal, notoriedad o por el simple deseo de ver que podían hacerlo. Los estados-nación constituyen la amenaza más dedicada y persistente. Los grupos de espionaje rusos conocidos como "*Fancy Bear*" (APT 28) y "*Cozy Bear*" (APT 29) estuvieron implicados en el hackeo de las campañas de EE. UU. en 2016. Los chinos se han concentrado mucho más en recopilar información. Se cree que estuvieron activos en las campañas presidenciales de EE. UU. de 2008 y 2012, pero no hay ninguna evidencia de que hayan publicado algún material hurtado. Por haber producido la película *The Interview*, Sony Pictures Entertainment recibió de Corea del Norte la infame represalia de robar y publicar correos electrónicos de la compañía, y borrar sus sistemas. En algunos países, las campañas de oposición pueden asimismo tener que enfrentar las amenazas de su propio gobierno. La intensificación de las tensiones internacionales (especialmente en torno a elecciones en las que hay mucho en juego) podrían en el futuro promover más ataques.

Cómo enfrentarse a los ciberriesgos

El riesgo se entiende mejor en tres partes. En primer lugar tenemos las vulnerabilidades: las debilidades de su campaña que hacen que la información sea susceptible al robo, la alteración o la destrucción. Ellas pueden tener su origen en el hardware, el software, los procesos y en el nivel de vigilancia de su personal. Luego existen las propias *amenazas*: los estados-nación, los *hacktivistas* y otros grupos no estatales con capacidad de aprovechar dichas vulnerabilidades. Los riesgos se presentan donde las vulnerabilidades se encuentran con las amenazas. Por último tenemos las consecuencias: el impacto cuando los actores maliciosos aprovechan al máximo un riesgo no mitigado.

No hay nada que usted o su campaña puedan hacer para prevenir prevenir estas amenazas; estas son el resultado de fuerzas mayores, económicas y sociales más grandes. Lo que sí puede hacer es reducir sustancialmente las posibilidades de que sus adversarios tengan éxito al reducir su vulnerabilidad. Al reducir las vulnerabilidades, se reduce el riesgo; usted decide cuáles son los más importantes que se deben reducir. Por ejemplo, podría decidir que el acto más dañino que un *hacker* podría cometer es robarle el informe de autoinvestigación de su candidato, por lo que dedicará más recursos a un almacenaje seguro en la nube, exigirá el uso de contraseñas largas y restringirá el acceso a unas cuantas personas. Podría decidir que otros documentos de la campaña estén más ampliamente disponibles y sean menos seguros, puesto que son más personas las que los necesitan para hacer su trabajo y no causarían mucho daño en caso de filtrarse. Adviértase que los pasos que las campañas toman para asegurar sus datos y responder a cualquier ciberincidente se encuentran también sujetos a las mismas leyes de protección y privacidad de los datos que están apareciendo por todo el mundo, como el Reglamento General de Protección de Datos (RGPD) en Europa.

Hay aspectos técnicos de mitigación del riesgo y, en este manual, tenemos muchas recomendaciones técnicas; sin embargo, lo más importante es su enfoque holista. Como dirigente de campaña, lo más importante que puede hacer es tomar decisiones fundamentales como, por ejemplo, decidir quién tiene acceso a la información, qué información guarda o elimina, cuánto tiempo le dedicará a la capacitación y su propio comportamiento como ejemplo a seguir. Como profesional en campañas, el manejo del riesgo, tanto técnico como humano, es su responsabilidad. Depende de usted decidir qué datos y sistemas son los más valiosos y qué recursos dedicará a protegerlos.

Cómo proteger su campaña

Nuestras recomendaciones de seguridad están organizadas según tres principios básicos:

1. Prepárese:

El éxito de casi todas las recomendaciones del manual depende de que los dirigentes de la campaña creen una cultura de vigilancia de la seguridad que minimice los eslabones débiles. Esto significa establecer reglas básicas claras que se hagan cumplir de manera descendente y a las que se adopte de manera ascendente.

2. Proteja:

La protección es crucial. Cuando descubra que tiene un problema de seguridad será ya demasiado tarde. Levantar las defensas más fuertes que el tiempo y el dinero permitan es clave para reducir los riesgos. La seguridad de la Internet y de los datos funciona mejor en niveles: no hay una sola tecnología o producto a prueba de balas. Unas cuantas medidas básicas usadas conjuntamente podrían hacer que la arquitectura digital de una campaña sea más difícil de filtrar, y más resiliente de quedar comprometida, lo que en última instancia le ahorrará tiempo y dinero a su campaña en el futuro.

3. Persista:

Las campañas ahora enfrentan adversarios con niveles mayores en recursos y de pericia; en la actualidad, ni la cultura más vigilante ni la infraestructura más fuerte podrían prevenir una violación de la seguridad. Las campañas necesitan desarrollar un plan con anticipación para hacer frente a una posible violación de seguridad.

Algunas campañas cuentan con más tiempo y dinero para la ciberseguridad que otras. Es por ello que nuestras recomendaciones ofrecen dos niveles de protección: "**bueno**" y "**mejorado**". El primer nivel "bueno" representa todo lo que una campaña debe hacer para tener un nivel mínimo de seguridad. Debe siempre aspirar a hacer más según lo permitan el tiempo, el dinero y las personas, razón por la cual recomendamos usar el nivel "mejorado" siempre que sea posible. Si tiene los recursos con que obtener un apoyo respetable y capacitado de TI, será dinero bien invertido. Las amenazas están evolucionando constantemente y los servicios profesionales de TI le ayudarán a ir más allá de lo que este manual ofrece, y a mantenerse al tanto de las últimas amenazas y soluciones para su caso.

Dirección

Los directores de campaña deben asumir la responsabilidad por su estrategia de ciberseguridad, pero la mayoría delegará su desarrollo y supervisión a un subdirector o a un director de operaciones. Es importante que la ciberseguridad esté firmemente integrada al trabajo en recursos humanos (RR. HH.) y tecnología de la información (TI), pues las formas correctas de incorporar personal, suministrar hardware y controlar los permisos serán algo crucial para su estrategia. Muchas campañas pequeñas dependen del apoyo de voluntarios en lo que respecta a la TI y la ciberseguridad. Puede usar este manual para guiar sus discusiones con su voluntariado. La clave es escudriñar exhaustivamente a los voluntarios que le apoyen y controlar cuidadosamente el acceso, de modo tal que no puedan crear nuevas vulnerabilidades. Asegúrese de que un miembro del personal de campaña supervise el trabajo en TI y controle los permisos para acceder a distintos sistemas.

Cuándo comenzar

La *ciberseguridad debe comenzar el primer día*, sea cual fuere el modelo de apoyo con el que cuente. A continuación aparece una "lista de las cinco medidas más importantes", las cuales son del todo cruciales. Asegúrese de que estén instaladas desde un principio aun en caso de solo tener dos miembros en su personal, y luego complete las demás recomendaciones "buenas" tan pronto sea posible. Pero si estas medidas no forman parte de su primer plan digital, no se preocupe. No es demasiado tarde para que adopte medidas de seguridad efectivas y proteger lo que ya está haciendo.

Costo

Gran parte de lo que recomendamos es gratuito o tiene un costo muy bajo. De hecho, todo en nuestra lista de las cinco medidas más importantes es gratis, excepto el conseguir una plataforma con base en la nube, lo que solo le costará unos cuantos dólares al mes por empleado. Las campañas con una meta alta necesitarán presupuestar suficientes recursos para hardware y software con que implementar una estrategia responsable, pero esto también también debiera ser solo un pequeño porcentaje del presupuesto de una campaña de varios millones de dólares. Las campañas más pequeñas podrán ejecutar nuestras recomendaciones con unos cuantos cientos a unos cuantos miles de dólares, dependiendo de cuánto personal o voluntarios trabajen en la campaña.

Toda referencia a proveedores y productos busca brindar ejemplos de soluciones comunes y no constituye un apoyo a algún producto. De surgir problemas al implementar productos o servicios, sugerimos que se ponga en contacto directamente con los proveedores, quienes usualmente

pueden brindar asistencia técnica al nivel del usuario. Cuando se trata de la selección de productos y servicios, sugerimos que toda campaña consulte con un experto en ciberseguridad o efectúe un estudio independiente para averiguar cuál es el mejor producto para sus necesidades.

Las Cinco Medidas Más Importantes

1. Establezca una cultura de conciencia de seguridad de la información:

Tome en serio la ciberseguridad. Asuma la responsabilidad por la reducción del riesgo, capacite a su personal y voluntarios, y dé el ejemplo. Los errores humanos son la causa número uno de las violaciones de seguridad.

2. Use la nube:

Uno de los grandes servicios comerciales en la nube será mucho más seguro que cualquier sistema que pueda armar con sus limitados recursos. Considere usar un paquete de oficina con base en la nube, como GSuite o Microsoft365, que le brindarán todas sus funciones básicas de oficina y un lugar seguro en donde guardar información (véase “Qué es la nube” en la p. 22).

3. Use autenticación de dos -factores (A2F) y contraseñas fuertes:

Exija autenticación de dos factores (A2F) para así agregar un segundo nivel de protección a todas las cuentas importantes, entre ellas su paquete de oficina, todo servicio de correo o de almacenaje y las cuentas de sus redes sociales. Para su segundo factor use una aplicación móvil o llave física, no mensajería de texto. Para sus contraseñas cree ALGOREALMENTELARGOCOMOESTEHILO, no algo realmente corto como 3$TO. Contra lo que se suele creer, un hilo largo de palabras aleatorias sin símbolos es más difícil de quebrar que algo corto con Much0$ S1mB0lo$. Jamás repita las claves; un gestor de contraseñas también puede ayudarle con esto, al permitirle generar aleatoriamente claves fuertes y auditar sus contraseñas ya existentes para identificar las que han sido usadas.

4. Use mensajería cifrada para conversaciones y materiales delicados:

Usar una herramienta de mensajería cifrada para celulares, como Signal o Wickr, con los mensajes y documentos confidenciales significa que los adversarios no podrán conseguirlos incluso si *hackean* su cuenta de correo electrónico. La codificación cifra los datos y reduce drásticamente la posibilidad de que alguien pueda leer sus mensajes incluso en caso de interceptar los datos.

5. Planee y prepare:

Tenga listo un plan en caso de que su seguridad quede comprometida. Sepa a quién llamar para pedir ayuda técnica, entienda sus obligaciones legales y esté listo para comunicarse interna y externamente tan rápido y eficazmente como sea posible.

Pasos para proteger su campaña

Paso 1: El elemento humano

La ciberseguridad esencialmente es un problema humano y no técnico. Las mejores soluciones técnicas del mundo no tendrán efecto alguno de no implementárselas correctamente, o si no se las actualiza continuamente a medida que la tecnología evoluciona. Las prácticas de ciberseguridad exitosas dependen de que se cree una cultura de seguridad.

BUENO — lo que debe hacer

1. Establezca una vigorosa cultura de protección que enfatice la seguridad como un criterio para una campaña vencedora. Así como se ordena al personal de campaña que no infrinja las normas de financiamiento de campaña, así también los empleados deben evitar hacer clic en enlaces o abrir archivos adjuntos en correo electrónicos de remitentes desconocidos.

    a. **Inmersión**: al incorporar personal nuevo, proporcione una capacitación básica en seguridad de la información. Durante su capacitación puede repartir el Folleto del personal.

    b. **Capacitaciones**: haga tal que la seguridad forme parte de todas sus capacitaciones de personal, como eventos del personal directivo o la capacitación de mobilizar el voto [get-out-the-vote (GOTV)] preelectoral. Proporcione capacitación adicional para quienes tienen funciones delicadas como el candidato, el personal de prensa, el personal directivo y todo aquel que tenga privilegios de administrador de sistema en su red. Los directores deben exigir que el director de TI (que podría ser el director mismo) revise las configuraciones de seguridad de las personas más importantes de la campaña, incluido el candidato. No sea tímido ni poco entusiasta en lo que se refiere a la seguridad del candidato y otros integrantes importantes de la campaña.

    c. **Dé el ejemplo**: el personal directivo de la campaña y el candidato deben asumir un rol de liderazgo visible y promover la ciberseguridad en las capacitaciones. El personal de más alto rango debe reforzar periódicamente la importancia de la ciberseguridad al personal de menor rango en reuniones y llamadas. No deje que sean solo los expertos técnicos los que se encarguen de las capacitaciones. El director de campaña o el de operaciones pueden ser mensajeros más impactantes, precisamente porque se les ve como menos “técnicos”.

2. Investigue exhaustivamente al personal, los voluntarios y los pasantes (y a todo aquel que solicite acceso a la información de la campaña) para así evitar dar credenciales a alguien que desee hurtar datos o sabotear sus sistemas.

a. Establezca una definición de lo que califica como información delicada y fije normas para su uso. Podría, por ejemplo, decidir declarar como “confidenciales” a todas las encuestas, materiales de investigación, memos de estrategia y los correos electrónicos del tema.

b. Prohíba la transferencia de información confidencial por canales de comunicación que no sean manejados y hayan sido protegidos por la campaña. Podría pedir que solo se la transfiera por mensajería cifrada (véa el Paso 2).

3. Confirme que los consultores y proveedores con acceso a la información confidencial cuenten con correo electrónico y almacenaje seguros (véa el Paso 2). En caso de alguna duda exija que usen una cuenta del paquete de oficina con base en la nube de la campaña (véase el Paso 2).

4. Controle el acceso a los servicios importantes en línea, como las cuentas oficiales de la campaña en las redes sociales, para así impedir su uso por parte de personas sin permiso. Asegúrese de que quienes dejen la campaña ya no tengan acceso a las cuentas relacionadas con esta. Puede hacer esto con facilidad empleando una herramienta de gestión de cuentas de redes sociales que actúe como puerta de enlace para todas sus cuentas. Cuando alguien deje la campaña deberá desactivar su cuenta de inmediato.

5. Explique al personal la amenaza del phishing. Asegúrese de que sepan cómo identificar y evitar enlaces sospechosos, y enfatice la importancia que tiene el identificar y denunciar los posibles ataques de phishing. Como parte de la vigorosa cultura de seguridad de la campaña, el personal directivo debe reconocer y felicitar a todo aquel que denuncie un comportamiento sospechoso en su sistema, o que admita haber hecho clic en un enlace potencialmente malicioso.

6. Entienda su entorno legal. En algunos lugares, la Unión Europea inclusive, los estándares de privacidad estipulan requisitos particulares para todo dato que su campaña pueda recabar, en especial la información personal, como los datos demográficos o las direcciones.

Handouts (Inglés)

» Para los miembros del personal
» Para los familiares

MEJORADO — dé el siguiente paso

1. El software como Phishme y KnowBe4 puede capacitar a su personal enviándoles correos electrónicos de phishing falsos. Esta es una forma segura, rápida y efectiva de saber quién está en riesgo de hacer clic en un enlace, para así capacitarles más. Muchos de estos productos también filtran algunos intentos de phishing de su correo electrónico.

2. Si tiene los recursos, contrate a un profesional de TI dedicado para que maneje los sistemas de su campaña, y a un experto en seguridad de TI para que ayude a proteger, mantener y monitorear la infraestructura digital de su campaña. Este puede ofrecer la capacitación y evaluación habituales del personal y los sistemas, al mismo tiempo que personaliza las soluciones de seguridad.

3. Contrate a una empresa de ciberseguridad para que brinde soluciones de seguridad, revise sus defensas y monitoree sus sistemas en busca de violaciones. Sepa a qué compañía contactar en caso de violación y requiera de un apoyo urgente para resolver el incidente. Esta es una alternativa a la contratación de un experto de seguridad de TI de tiempo completo. Haga su investigación y quédese con una compañía de altísima reputación: no todas las empresas de ciberseguridad ofrecen el mismo nivel de servicio.

CÓMO TRABAJAR CON PROFESIONALES DE SEGURIDAD

De decidir trabajar con un profesional de seguridad, ¿cómo evaluará a la persona o compañía correcta? Es importante que evite un apoyo costoso pero ineficaz, ya sea debido a recomendaciones personales o reseñas públicas positivas. Cuando entreviste a posibles profesionales en seguridad, pregúnteles cómo respondieron en el pasado a incidentes de este tipo y cómo hicieron posible que otros trabajaran con mayor seguridad. El comité nacional de su partido, o los profesionales de campaña de confianza, podrían recomendarle opciones entre las cuales escoger. Tenga en cuenta que la cultura afecta la seguridad, y que hasta las mejores recomendaciones podrían no tener resultado en caso de no hacer un seguimiento (i.e., tan solo contratar una compañía no resolverá sus problemas).

Paso 2: Comunicación

No todos los métodos de comunicación son igualmente seguros, así que debe ser consciente de cómo se comunica. La dirigencia de la campaña debe fijar una norma que incentive las conversaciones en persona cuando sea posible, y que desaliente el envío de correos electrónicos innecesarios o superfluos. Todo lo que escriba en uno de ellos podría ser publicado en la prensa o en las redes sociales, tal vez luego de una modificación maliciosa. Distintos productos y servicios ofrecen niveles diferentes de protección, trátese de llamadas telefónicas, mensajes de texto o correo electrónico, así que investigue antes de elegir qué sistemas habrá de usar su campaña.

BUENO — lo que debe hacer

1. Use los sistemas más seguros que pueda para sus comunicaciones.

    a. Use servicios de mensajería cifrados de extremo a extremo, como Signal o Wickr, en especial para enviar mensajes, compartir documentos y hacer llamadas telefónicas. Muchas campañas exigen que la información sensible solo se transmita mediante mensajería cifrada, y para el personal a menudo es más fácil acostumbrarse a emplear estas aplicaciones en toda comunicación de rutina (esto es especialmente útil en el caso de personas de alto riesgo, como el candidato). Signal y Wickr publican su código fuente para que se le examine y brindan funcionalidades que reducen los riesgos, como permitirle borrar los mensajes automáticamente. Asegúrese de que sus mensajes no se estén sincronizando con su computadora o con cuentas en la nube no cifradas.

    b. Desactive el archivado en servicios de mensajería como Google Chat y Slack, de modo tal que los chats viejos no puedan robarse posteriormente. Esto requiere entrar a “configuración” y ajustar las líneas de tiempo de la “política de retención”. Algunos servicios exigen que usted haga esto para toda conversación de chat. Recomendamos conservar los mensajes de chat por una semana o menos.

2. Use un paquete de programas para oficina basado en la nube, que brinde de forma segura comunicación de correo electrónico, creación de documentos, chat y uso compartido de archivos, como GSuite o Microsoft365. Por ejemplo, GSuite incluye Google Drive para compartir archivos, Gmail como servidor de correo electrónico, Google Hangouts para chat y Google Docs como procesador de texto, hojas de cálculo y presentaciones. Microsoft365 brinda OneDrive/SharePoint para compartir archivos, Outlook/Exchange para correo electrónico, Microsoft Teams para chat y Microsoft Office para procesador de texto, hojas de cálculo y presentaciones. Salvo que contrate profesionales en seguridad altamente experimentados (y potencialmente costosos), los sistemas con base en la nube, manejados por empresas importantes, estarán mejor protegidos que cualquier servidor que

usted pueda montar en su campaña. Hay versiones gratuitas de ambos productos, pero las versiones pagadas brindan más capacidades administrativas. Google también ofrece servicios gratuitos para proteger organizaciones en entornos amenazantes como Outline, una RPV autoalojada (*self-hosted VPN*); Project Shield, un servicio para proteger su página web de todo ataque para incapacitarla; y Password Alert, que le advierte cuando ingresa su contraseña de Gmail en una página de *phishing*.

3. Borre sus correo electrónicos

    a. Active el autoborrado de mensajes viejos en su aplicación de correo electrónico, para así reducir el número de mensajes que podrían robarse. Esto suele requerir el ingreso a la "configuración" y la modificación de la "política de retención" a periodos más cortos. Para asegurarse de que los mensajes no se queden en una carpeta de "correo borrado", ajuste la configuración para eliminarlos automáticamente de esta carpeta después de cierto tiempo. Recomendamos conservar los mensajes por un mes o menos, salvo que esté legalmente obligado a hacerlo por más tiempo. No pueden robarle lo que no tiene.

4. Proteja las cuentas personales

    a. Los asuntos de campaña jamás deben ir a cuentas personales. Sin embargo, los adversarios pondrán la mira en ellas para *hackearlas*, así que haga que su personal también emplee contraseñas fuertes y de dos factores en sus cuentas personales (esto se incluye en nuestro Folleto para el personal).

¿QUÉ ES LA NUBE?

Los “servicios en la nube” proporcionan manejo y acceso a información almacenada remotamente en Internet. Se ejecutan en servidores externos manejados por terceros; esto incluye a muchos servicios comunes que tal vez ya esté utilizando, como Gmail o Dropbox. Es bueno guardar la información en un proveedor confiable de servicio en la nube y no en su computadora personal, pues estos proveedores cuentan con el dinero, los recursos técnicos y los conocimientos para hacer que sus servidores sean más seguros que el disco duro de su equipo portátil o de un servidor de oficina. También cuentan con bastante personal técnico que trabaja defendiendo sus redes (y, por ende, también a sus datos) de ataques sofisticados. Es como la diferencia entre dejar dinero bajo su colchón y guardarlo en la bóveda de un banco. Utilizar servicios en la nube brinda una barrera adicional contra la pérdida de datos en caso de que un aparato individual se pierda o quede comprometido. El almacenaje en la nube es una característica incluida en servicios de seguridad de los paquetes de aplicaciones para oficina como GSuite y Microsoft365. Otros servicios son Dropbox o Box. Es importante tener en cuenta que estas corporaciones internacionales podrían estar sujetas a pedidos judiciales del historial de contactos, correos electrónicos o del contenido de los archivos. La mayoría de las principales corporaciones, entre ellas cualquiera de las aquí nombradas, tiene políticas estrictas de cuándo acatarán tales pedidos..

¿QUÉ SUCEDE SI NO CONFÍO EN LA NUBE?

Algunas organizaciones no están cómodas con la idea de confiar su información a un tercero. Si insiste en manejar su propia infraestructura tecnológica, sea consciente de que tendrá que defenderse de las fuerzas de seguridad de estados-nación. Algunas consideraciones:

- Usted será responsable de comprender, proteger y parchar todos los aspectos de sus sistemas, incluidos los sistemas operativos, las aplicaciones del servidor, el software mismo, las bases de datos y las tecnologías de conexión.
- Usted tendrá que asegurarse de que la conexión a sus plataformas claves sea sumamente confiable y no vulnerable a la manipulación, la censura o el DDoS ("denegación de servicio distribuidos" o DDoS por sus siglas en inglés).
- Usted tendrá que monitorear activamente en busca de ataques informáticos y hacer que alguien responda todo el día, todos los días.
- Usted tendrá que manejar copias de respaldo seguras externas.
- Si está en riesgo de un saqueo físico, se le podría robar toda su información.

¿QUÉ ES EL CIFRADO?

El cifrado es una forma de codificar la información cuando viaja entre usuarios o cuando se la almacena, de modo tal que no pueda leerla nadie salvo el receptor deseado. Mírelo de este modo: un usuario "codifica" los datos cuando los envía y solo el receptor deseado tiene la clave para descodificarlos. Usar cifrado es inteligente, especialmente en el caso de información confidencial, puesto que, incluso si los adversarios robaran los datos, sería improbable que puedan leerlos. La mayoría de las aplicaciones que usan cifrado, como Signal o Wickr, hacen que el proceso esté libre de interrupciones. El cifrado de extremo a extremo es una característica importante de los programas de comunicación: significa que su mensaje es secreto desde su teléfono o computadora hasta su destinatario inclusive, y que nadie (ni siquiera el proveedor mismo de la aplicación) puede leer los mensajes. De ser posible, use también el cifrado de todo el disco en su equipo portátil; en caso de robo o si se la olvida en un bus, nadie podrá leer su contenido.

CENSURA, VIGILANCIA Y CIERRES DE INTERNET

Lamentablemente, en muchas partes del mundo hay una tendencia creciente a controlar el uso de Internet como un espacio abierto y democrático. Esto podría incluir el bloqueo de canales de comunicación claves como, por ejemplo, WhatsApp o Twitter; la censura de sus páginas web públicas, o el espionaje agresivo a los ciudadanos que visitan sus propiedades en línea y lo que su personal hace en la web. En los casos más graves, que han aumentado de modo alarmante, un país puede cortar íntegramente el acceso a Internet.

Siempre cuente con un plan de respaldo. Si su partido o campaña es particularmente dependiente de su página web, asegúrese de que su página en Facebook tenga la información más importante en caso de que su página web sea bloqueada o censurada. Si WhatsApp es un canal de comunicación clave, esté preparado para usar SMS o tenga un árbol telefónico de respaldo con todos los números. Si monitorear el tráfico en la web o las actividades en línea de su personal de campaña pueden causar problemas, considere emplear herramientas de evasión o de anonimización como Tor Browser,[1] Psiphon[2] o la RPV personalizada de Outline.[3] Tenga a la mano su lista de periodistas y ayúdeles, en el caso de cambios importantes en la censura o el cierre de Internet, a hacer que esto mismo sea la noticia.

1. https://www.torproject.org/projects/torbrowser.html.en
2. https://www.psiphon3.com/en/index.html
3. https://getoutline.org/en/home

CÓMO MANTENER SUS PÁGINAS WEB EN LÍNEA

La página web de su campaña probablemente es una de sus plataformas de comunicación pública más importantes, y una de las formas más fáciles para que los ciudadanos le encuentren. Esto hace que su presencia en línea sea un blanco irresistible para hackers maliciosos o rivales inescrupulosos. Considere usar una plataforma de alojamiento administrado (managed hosting platform) como Wordpress.com, Wix o Google Pages, donde usted no tiene la responsabilidad de ser el administrador de seguridad de una página web. Si desea manejar su propia página, asegúrese de ser un experto, o de contratar profesionales para que la mantengan segura de los hackers.

Los atacantes cada vez usan más los ataques de “denegación de servicio distribuidos” (DDoS) para dejar una página fuera de línea durante periodos críticos mediante volúmenes inmensos de pedidos falsos. Las Redes de Distribución de Contenido (CDN) son capaces de conservar una copia en caché de su página en servidores poderosos que hay en todo el mundo, lo que hace que sea casi imposible bajarlas a todas. Dos productos que cuentan con la capacidad de asistirle protegiendo sus páginas web públicas son Cloudflare y el Project Shield de Google.

Paso 3: Acceso y manejo de cuentas

Uno de los aspectos más difíciles de la seguridad es mantener fuera a personas no autorizadas. Esto significa prevenir que los adversarios logren acceder a sus datos e impedir que gente dentro de su propia campaña tenga acceso a información que no necesita. Aunque algunas de las recomendaciones que aparecen a continuación podrían parecer engorrosas, los *hackers* dependen de quienes valoran la comodidad por encima de la seguridad.

¿QUÉ ES LA AUTENTICACIÓN DE DOS FACTORES?

La autenticación de dos factores es una una segunda capa de seguridad que requiere que un usuario presente una segunda credencial más allá de su contraseña. El segundo factor es crucial porque, de robarse su contraseña, un adversario no podrá ingresar a su cuenta. Su clave es algo que usted sabe y el segundo factor es algo que usted tiene, como un código generado por una aplicación, una llave física o incluso un dato biométrico, como una huella digital.

BUENO — lo que debe hacer

1. Requiera autenticación de dos factores (A2F) en todos sus sistemas y aplicaciones. Evite los mensajes de texto (SMS) en ella porque los atacantes pueden fácilmente clonar un número telefónico y acceder a los textos. Hay varias aplicaciones de A2F que funcionan igual de bien que los SMS, como Google Authenticator, Microsoft Authenticator y Duo Mobile. También puede usar una clave de "identidad rápida en línea" FIDO ("fast identity online") física que se inserta en el puerto USB, como Yubikey o Feitian. La página web "TwoFactorAuth.org" es una guía útil de los servicios que ofrecen y no ofrecen A2F.
2. Contraseñas.
    a. Exija contraseñas fuertes. Como ya señalamos, "use contraseñas que sean largas y fuertes". Las actuales capacidades cibernéticas pueden romper una clave de siete caracteres en milisegundos. Una clave de 20 o hasta 30 caracteres hará que le tome a un hacker mucho más tiempo quebrarla. Elija una serie de palabras que pueda recordar fácilmente.
    b. ¡No repita contraseñas! Use una clave distinta en cuentas diferentes, de modo tal que un hacker no pueda entrar a varias cuentas en caso de robar una sola contraseña.

c. Para proteger al personal y a los voluntarios de la campaña de ataques de phishing, solo comparta contraseñas en persona o en mensajes cifrados de corta duración. Exija que el cambio de las claves de las cuentas centrales se solicite usando estos mismos métodos o en un videochat, para así asegurarse de que realmente se trate del personal o los voluntarios de la campaña. Jamás comparta contraseñas por correo electrónico o guárdelas/distribúyalas usando un sistema de soporte técnico.

3. Use un administrador de contraseñas como LastPass, 1Password o Dashlane para que le ayude a manejar con facilidad muchísimas claves largas y fuertes. Pero asegúrese de que su sistema de gerenciamiento tenga una contraseña larga y fuerte, y autenticación de dos factores. Actualmente no recomendamos administradores de contraseñas incorporados a navegadores tales como Chrome, Safari y Firefox, que suelen ser menos seguros que estos administradores independientes.

4. Cree cuentas separadas para administradores y usuarios, y restrinja severamente el acceso a las primeras. Los administradores deben asimismo tener cuentas de campaña separadas, una solo para sus labores administrativas y otra cuenta de usuario estándar para todos los asuntos restantes de la campaña. Esto reducirá la posibilidad de que un adversario logre comprometer una cuenta de administrador, lo que daría acceso a toda la red.

5. Efectúe revisiones periódicas de quién tiene acceso a distintos dispositivos y redes. Bloquee de inmediato el acceso de quienes dejen la campaña. Cambie las contraseñas de inmediato en caso de observarse actividades sospechosas. Para que esto sea posible, asegúrese de que su personal no esté compartiendo cuentas de usuario.

ADMINISTRADORES DE CONTRASEÑAS

Los administradores de contraseñas son una forma de guardar, recuperar y generar claves. Algunos hasta tienen la capacidad de completar automáticamente la línea de contraseña en las páginas de ingreso. El administrador de contraseñas requiere de su propia clave para ingresar, y esta se convierte en la única que tiene que recordar. El riesgo, claro está, es que si alguien ingresa a su administrador (ha sucedido), esa persona tendrá todas sus contraseñas. Pero este riesgo casi siempre queda compensado con el beneficio de las claves fuertes y únicas en todas sus cuentas, y se le puede reducir considerablemente con la autenticación de dos factores en su administrador de contraseñas. Para una campaña, los administradores de contraseñas a veces tienen sentido en el caso de cuentas con varios usuarios, pues el administrador permite compartir el acceso a ellas con seguridad.

MEJORADO — dé el siguiente paso

1. Cree perfiles de usuario para los distintos tipos de personal de campaña, que automáticamente otorguen el nivel de acceso necesario. Distintos tipos de empleados (voluntarios, pasantes, personal de campo, dirigencia de la campaña) necesitan acceder a distintos recursos. Contar con perfiles predeterminados hace que sea más fácil asegurarse de que las personas tengan acceso solo a lo que necesitan.

¿QUÉ SON LOS ADMINISTRADORES?

En lenguaje de TI, un "administrador" o "admin" tiene la capacidad de dar a las personas acceso a los sistemas o la información, o control sobre ellos. Por ejemplo, como "admin" de un sistema de correo electrónico usted puede crear cuentas, cambiar contraseñas y fijar requisitos tales como la longitud de las claves y la autenticación de dos factores para todas las cuentas. En un conjunto de herramientas de oficina como GSuite o Microsoft 365 también puede crear grupos, como "Equipo de campo" o "Equipo de Comunicaciones". El trabajo de un Admin es realmente importante. Si hace las cosas bien, la información estará a disposición solo de quien la necesita, lo cual es esencial para la seguridad. Esto significa que decidir quién habrá de tener los privilegios de Admin es también una decisión crucial. Solo unas cuantas personas sumamente confiables y capacitadas deben poder otorgar a otros el acceso a la información. Si un miembro del personal con privilegios de "admin" deja la campaña, asegúrese de retirarle sus privilegios de inmediato!

Paso 4: Planificación de las repuestas a los incidentes

Planificar cómo responder a un ataque es igual de importante que diseñar una estrategia de seguridad con qué prevenirlos. Cómo responda tendrá más que ver con el resultado final de un incidente, que con lo que quedó comprometido. Deberá presupuestar algo de tiempo con la dirigencia o la dirección más alta para discutir qué sucederá si algo sale mal. Aquí tenemos una lista de los pasos que debe tomar:

LEGALES

Identifique abogados externos a los cuales contratará en caso de un ciberincidente, y discuta con ellos el proceso de respuesta al inicio de la campaña. En la mayoría de los casos esta será la misma persona que representa a su campaña en otros asuntos, pero idealmente debería tener disponible a alguien que se especialice en responder a incidentes, ya sea pro bono o por un adelanto de $0.

Pídale a su abogado que le explique sus obligaciones legales en caso de hurto de datos, y con qué medidas de cumplimiento deberá contar.

Entienda la obligación legal de sus proveedores de notificarle a usted o a otros si han sido hackeados. De ser posible incluya un estricto requisito de notificación en sus contratos con ellos, pues los terceros son una frecuente fuente de violaciones de seguridad.

Si cree que ha sufrido una violación de seguridad, una práctica adecuada es que su abogado supervise su respuesta bajo el privilegio de confidencialidad entre abogado y cliente.

Converse con su abogado acerca de la mejor forma de trabajar con los cuerpos policiales en caso de violación de seguridad. Cada campaña lo hará de distinto modo.

TÉCNICAS

Establezca por anticipado a quién pedirá asistencia técnica si cree que ha sido *hackeado*.

Elija alguien de la campaña para que interactúe con los expertos técnicos en caso de una violación de seguridad. Idealmente será la misma persona que ya está coordinando la TI para la campaña. Manejar la respuesta a un incidente puede ser abrumador, por lo que querrá tener alguien que se concentre en los aspectos técnicos y sepa lo que está haciendo. De este modo usted podrá concentrarse en comunicarse con las partes interesadas y con la prensa.

Entérese de la asistencia técnica u otro apoyo que los proveedores de plataforma puedan brindarle en caso de un ciberincidente, como un hackeo u otro tipo de ataque.

OPERACIONES

Decida por adelantado quiénes estarán en su Equipo de Respuesta a Incidentes (ERI) y quiénes tomarán parte en las reuniones de respuesta a incidentes. Es importante incluir a un integrante de sus equipos de TI, legal, operaciones y comunicaciones. Si la campaña es pequeña y no tienen apoyo a tiempo completo en comunicaciones, TI u operaciones, planifique incluir a todo miembro clave del personal que supervise las operaciones de la campaña.

Establezca la cadena de mando de toma de decisiones en caso de una violación de seguridad, especialmente en lo que se refiere a comunicaciones. En muchos casos este será el director de campaña, pero algunos directores podrían elegir delegarle la responsabilidad a otra persona.

Identifique qué aplicación o tecnología usará para comunicarse si cree que sus sistemas han sufrido una violación de seguridad. Por ejemplo, si su correo electrónico fue *hackeado*, tal vez quiera depender de una aplicación de mensajería segura como Signal o Wickr. La comunicación durante estos incidentes es esencial, pero no querrá que sus adversarios sepan qué está diciendo, o incluso que ya está respondiendo a sus actos.

COMUNICACIONES

Efectúe una planificación de la situación. En el caso de muchas campañas esto podría formar parte de un retiro de estrategia ya existente. Para las campañas más grandes con mayor riesgo podría ser necesario tener una reunión dedicada a ello.

Identifique a las partes interesadas claves tanto internas como externas, como su personal, voluntarios, donantes y partidarios. Sepa a quiénes debe contactar de darse un incidente y clasifíquelos por orden de prioridad. Arme una lista de contactos y designe quién se comunicará con ellos.

Efectúe una lluvia de ideas con las situaciones más dañinas y considere cómo podrían cambiar las partes interesadas y su mensaje en cada caso. Las distintas situaciones podrían incluir:

- Corren rumores de que su campaña ha sido *hackeada*;
- Se filtra la información personal de los partidarios;
- Se roban la información financiera confidencial de los donantes, como números de tarjetas de crédito e información de contacto;

- Se instala *ransomware* y se intenta extorsionar a su campaña;
- Se borran y apagan sus sistemas;
- Se roban los correo electrónicos de alguien;
- Su adversario roba las credenciales de su administrador y todo archivo del disco de su campaña;
- Cierran o *hackean* sus cuentas en las redes sociales;
- Se corta Internet, o sitios, aplicaciones o protocolos particulares quedan bloqueados a nivel nacional;
- El acceso a información crítica queda bloqueado o interrumpido por la censura.

Tenga cuidado con lo que dice sobre la política de ciberseguridad o los ciberincidentes. Algunas víctimas del cibercrimen habían efectuado pronunciamientos grandiosos acerca de sus propias medidas de seguridad, o habían criticado a otros que habían sido atacados. De ser víctima, la prensa le responsabilizará por lo que dijo antes.

De igual modo evite dar detalles acerca del alcance del incidente durante las primeras fases (y tanto mejor si puede evitar discutir del todo su alcance). Los detalles disponibles al principio cambiarán a medida que investigue. Un error común es decir algo que posteriormente resulta no ser cierto (v.g., “no robaron mucho”, o “no tomaron información personal”). El curso más seguro es decir solo lo que sabe con toda seguridad. Las declaraciones deben concentrarse en las medidas que está tomando para remediar la situación para las partes interesadas que se han visto afectadas.

Prepare algo de lenguaje estandarizado por adelantado, idealmente en consulta con sus representantes legales, de modo tal que pueda redactar rápidamente declaraciones o temas de discusión de darse un incidente. Como mínimo cree un documento simple de preguntas y respuestas (P y R) que pueda revisar rápido cuando realmente lo necesite. Crear uno de estos documentos por adelantado le ayudará a pensar tanto sobre lo que no dirá como sobre lo que sí mencionará. Por ejemplo, la primera pregunta frecuentemente será “¿Qué sucedió?”. Pero es posible que no pueda responderla durante días o semanas. El hecho de que no puede saber por anticipado qué tipo de violación de seguridad tendrá lugar puede en realidad ayudarle a preparar mejores respuestas de lenguaje estandarizado por adelantado.

LAS PREGUNTAS QUE DEBE INCLUIR EN SU DOCUMENTO DE P Y R SON:

- What happened?
- How did it happen?
- Who did it?
- What was stolen or damaged?
- Was anyone's personal information stolen? What are you doing to protect them?
- How did the hackers do it?
- Are the hackers out of your system?
- How long were they in your system?
- What security measures did you have in place? Why weren't they effective?
- Shouldn't you have known this would happen? Why weren't your systems better secured?
- Are you working with law enforcement? Has law enforcement contacted you?
- In a ransomware breach, you'll be asked: Did you pay the ransom and why or why not?

Manténgase en contacto con sus principales partes interesadas y manténgalas tan informadas como pueda. Probablemente no podrá decir mucho, pero es clave contactarles regularmente con lo que sabe, contar con una declaración clara de sus intenciones y brindar detalles acerca de lo que están haciendo para hacer frente a la situación. Evite fijar la expectativa de actualizaciones demasiado frecuentes, pues a menudo no contará con nueva información y sus partes interesadas quedarán frustradas si regresa a ellos sin algo nuevo. Solo hable proactivamente a los medios si tiene nueva información que proporcionar.

Paso 5: Dispositivos

Todo aparato físico de su campaña, desde un celular, tableta o laptop hasta un enrutador, impresora o cámara, es una posible vía de ataque a su red. Un buen plan de ciberseguridad intentará controlar el acceso a todos sus dispositivos. Usted puede controlar el acceso a todos los dispositivos asegurándose de que siempre se les maneje bien y estén contabilizados. Puede controlar el acceso a los dispositivos mediante una autenticación de dos factores y contraseñas fuertes. Su contenido se controla mediante el cifrado y las políticas que guían cómo guardar los datos (esto es, el almacenaje de la información en la nube y no en las máquinas).

BUENO — lo que debe hacer

1. Siempre use el sistema operativo (SO) más actualizado posible, pues las actualizaciones del sistema incluyen regularmente parches para las vulnerabilidades más recientes. De ser posible, configure el aparato para que instale automáticamente dichas actualizaciones. Haga que alguien se encargue de revisar con regularidad que todos estén actualizados.

2. Haga una copia de respaldo. Asegúrese de contar con un plan de copia de seguridad para todos los datos que tenga guardados en un aparato local (su equipo de escritorio, por ejemplo) en caso de robo físico, de que su computadora se rompa o de que vierta café sobre el teclado. Podría, por ejemplo, usar un servicio de respaldo automático con base en la nube para así mitigar el impacto de la pérdida de datos. Entre los ejemplos tenemos a Backblaze y CrashPlan.

3. Acceso al dispositivo

    a. La dirigencia de la campaña debe crear desde el principio un entorno en el cual las personas tomen en serio la seguridad física de sus dispositivos; perder uno podría darle a un adversario el acceso a información crucial que podría usarse para dañar la campaña.

    b. Si bien es cierto que para muchas campañas no se pueden comprar dispositivos nuevos, de poderse siempre será mejor adquirir equipos nuevos (en especial computadoras y teléfonos). Como mínimo debe proporcionar equipos nuevos para el personal que trabaja con datos confidenciales, o cuando menos borrar y volver a instalar el sistema operativo en los aparatos viejos. Si el personal está usando sus propios equipos y teléfonos, establezca una política de “traiga su propio dispositivo” (BYOD,Bring Your Own Device) que implemente fuertes prácticas de seguridad (véase protección de terminales más adelante).

    c. Los miembros de la campaña NO deben usar cuentas de correo electrónico ni dispositivos personales en asuntos de campaña que no hayan sido protegidos siguiendo la política de BYOD, incluidos el correo electrónico y las redes sociales. Toda información importante

almacenada en dispositivos externos o sistemas controlados por la campaña será vulnerable a un ataque. Los dirigentes deben reiterar constantemente que los datos de campaña deben permanecer fuera del correo personal y los equipos sin seguridad.

d. Mantenga la seguridad física de sus dispositivos. Cuando use el transporte público, esté en un café o incluso en su oficina, siempre tome medidas para impedir el robo de dispositivos que pudieran dar acceso a sus cuentas, comunicaciones y datos.

e. Denuncie la pérdida de dispositivos de inmediato. Exija configuraciones por defecto que permitan borrarlos todos a distancia. Entre los ejemplos tenemos Buscar mi iPhone y Android Device Manager.

f. Gane o pierda, tenga listo un plan para lo que habrá de hacerse con todos los datos, cuentas y dispositivos una vez terminada la campaña. El periodo inmediatamente posterior a la campaña es particularmente vulnerable.

4. Acceso a los dispositivos

a. Cambie las contraseñas y la configuración por defecto en todos los dispositivos. Muchos de estos vienen de fábrica con una contraseña por defecto que es realmente fácil de adivinar. Desactive, además, la cuenta invitada si el dispositivo viene con una de ellas.

b. Implemente el cierre automático para los teléfonos y los equipos después de dos minutos, y para abrirlos exija una contraseña o identificación con huella digital.

c. Active el borrado automático en sus dispositivos móviles, de modo tal que se borren solos luego de cierto número de intentos de ingresar fallidos.

5. El contenido en los dispositivos

a. Exija el cifrado de todos los dispositivos (equipos y teléfonos), para así asegurarse de que la pérdida de uno de ellos no signifique que su contenido quede comprometido. Ejemplos de ello son FileVault para Mac y BitLocker para Windows. Algunos dispositivos como el iPhone hacen esto por defecto, pero no todos.

b. Instale software de protección de terminales en todos los dispositivos. Algunos ejemplos de ello son Trend Micro, Sophos y Windows Defender. Hay aplicaciones especiales de seguridad de terminales para teléfonos y tabletas, como Lookout.

¿QUÉ ES LA PROTECCIÓN DE TERMINALES?

Los terminales son los dispositivos que el personal usa, incluidos celulares, equipos portátiles y de escritorio. Son los "terminales" de la red de la campaña y el personal son los "usuarios finales". La protección de los terminales controla y maneja centralmente la seguridad en los dispositivos remotos. Es particularmente importante que las campañas permitan al personal "llevar sus propios dispositivos" (*BYOD*), puesto que ella necesita asegurarse de que estos sean seguros, que estén libres de malware y que puedan borrarse en caso de pérdida o robo. La protección de los terminales puede asimismo monitorear el dispositivo para asegurarse de que el software esté actualizado y detectar nuevo malware o posibles amenazas. Para muchas campañas esto parecerá ser un esfuerzo exagerado, pero incorporarla a su rutina de inmersión e invertir algo de tiempo por anticipado podría ahorrarle bastantes problemas posteriormente.

MEJORADO — dé el siguiente paso

1. Use software de gestión de dispositivos móviles (MDM), que monitorea la actividad, para asegurarse de que todos los dispositivos cumplan con las políticas de seguridad de celulares y dispositivos móviles que haya establecido para su campaña. Son ejemplos de ello VMware AirWatch, Microsoft InTune y JAMF. GSuite y Microsoft Office 365 también incluyen un servicio de MDM.

2. Use servicios de protección avanzada contra amenazas que monitoreen y alerten de actividades maliciosas, como CrowdStrike Falcon o Mandiant FireEye. Crowdstrike a veces ofrece el servicio Falcon de prevención de violaciones de seguridad pro bono a través de la Crowdstrike Foundation, dependiendo de las necesidades de su campaña y de las reglas de financiamiento de la misma.

Paso 6: Redes

Las redes son el sistema de hardware físico, software digital y sus conexiones. Representan otro rico entorno en blanco que atacar. Seguridad de la red compromete todo, desde cómo se comunican los dispositivos entre sí, hasta el uso de servicios en la nube para guardar datos.

BUENO — lo que debe hacer

1. Almacene datos en servicios de confianza en la nube, no en equipos personales o servidores. Todo lo que esté guardado en un dispositivo personal enfrenta un mayor riesgo de hackeo, robo, accidentes o incursiones que los datos almacenados en la nube.
    a. Nadie debe tener acceso a todos los archivos de la red; las cuentas con un acceso total de administrador no deben usarse en el trabajo diario. Divida sus archivos almacenados en carpetas departamentales y otorgue acceso en conformidad a ello.
    b. Asegúrese de que el acceso al contenido compartido lo sea solo por invitación. Algunos servicios de administración de archivos también permiten implementar fechas de vencimiento a las invitaciones y el acceso.
    c. Audite periódicamente qué se está compartiendo y con quién.
2. Tenga una red de wifi de "invitados" distinta para visitantes y voluntarios, que limite su acceso a los recursos de la campaña. Intente comprar enrutadores que ofrezcan un "perfil de invitado" que segmente su red automáticamente. Sugerimos vigorosamente que cambie la contraseña de la red al finalizar los eventos de la campaña, cuando podría darse una gran rotación del personal.
3. Evite lo más posible los servicios públicos de wifi cuando viaje o antes de armar su oficina de campaña, y siempre que sea posible emplee redes de wifi confiables. De necesitar wifi móvil intente brindarle a su personal de campaña hotspots de wifi para su anclaje. El wifi público a menudo es gratuito y fácil de conectarse, pero los atacantes también pueden usarlo para penetrar en su hardware.
    a. Cuando sea posible, el personal debe usar una RPV (red privada virtual). Estas ayudan a protegerse de los intrusos cuando se está en el wifi público. Algunos ejemplos de servicios de RPV son ExpressVPN o TunnelBear. No todas las RPV son creadas iguales. Cuídese de los servicios gratuitos: muchos buscan capturar sus datos.
4. Secure your browser. PC Magazine ranked Chrome and Firefox as the two safest browsers in 2017. Regardless of what browser you use, keep it up to date.

¿QUÉ SON LAS RPV?

Una red privada virtual (RPV) es un "túnel" cifrado para el tráfico en Internet, que lo esconde de los intrusos. Algunas oficinas las usan como una forma de ingresar remotamente a su red, pero esto no es muy común en las campañas. Estas deben considerar hacer que su personal use una RPV en los equipos y los teléfonos móviles si frecuentemente tienen que usar wifi público o redes no confiables (suele ser el caso del personal que viaja o en las oficinas de campo). Google recientemente lanzó un nuevo sistema de RPV personalizada llamado Outline.

MEJORADO — dé el siguiente paso

1. Puede tomar medidas más avanzadas para proteger su red, pero debe implementarlas un profesional de TI. Sugerimos que le pida que incluya lo siguiente:
    a. Usar un firewall de hardware.
    b. Cifrar su conexión de wifi con los protocolos de seguridad WPA2 o 802.1x (no use WEP).
    c. Configurar proxies web basados en la nube para así bloquear el acceso a sitios sospechosos desde cualquier dispositivo de propiedad de la campaña, esté donde esté. Entre los ejemplos de proveedores de servicio tenemos a Zscaler, Cisco Umbrella y McAfee Web Gateway Cloud Service.
    d. Hacer que su registro de actividad se guarde en un proveedor de servicio en la nube, como LogEntries o SumoLogic.
    e. Segmentar su almacenaje basado en la nube para que de este modo no todo esté guardado en el mismo lugar. Los estudios de la oposición, los memos de estrategia y los archivos del personal deben guardarse en carpetas diferentes, y el acceso a ellas debe quedar restringido a las personas que realmente los necesitan. Considere un sistema de almacenaje del todo distinto para la información más confidencial de su campaña. Restrinja el acceso de modo que solo el personal clave pueda acceder a ella, y solo usando dispositivos específicos. (Por ejemplo, si usa Microsoft365 como su suite de oficina y almacenaje de documentos, coloque la documentación más sensible en una cuenta de Dropbox o Box.) Esta segmentación podría limitar los daños de quedar comprometido un miembro de la campaña.
2. Entrene al personal para que no conecte sus dispositivos a puertos o dispositivos desconocidos. No use cargadores públicos en aeropuertos ni eventos. No acepte cargadores ni baterías gratuitos para teléfono en eventos (esa memoria USB gratuita podría estar cargada de malware).

Paso 7: Operativos de información y comunicaciones de cara al público

Los operativos de información recientemente han aparecido bastante en las noticias, especialmente en las campañas dirigidas por servicios de inteligencia extranjeros. Dependerá de los líderes electos y de los formuladores de política decidir cómo enfrentar a estos operativos al avanzar, y como personal de campaña es poco lo que podemos hacer para tener un impacto sobre si tienen lugar o no, pero sí hay unas cuantas cosas que podríamos hacer para manejarlos en caso de que se den. Las campañas son y seguirán siendo blanco de estas operaciones y necesitan estar preparadas. Defender cómo es que su campaña se comunica con el público forma parte importante de esto. A continuación figuran algunas formas con que protegerse mejor de operativos de información, identificar cuándo le estén sucediendo a su campaña o candidato, y responder rápidamente cuando sucedan.

¿QUÉ SON LOS OPERATIVOS DE INFORMACIÓN?

La información es poder, o al menos eso es lo que piensan muchos militares y servicios de inteligencia. El poder de las ideas hace tiempo que alimenta rebeliones, insurgencias y guerras civiles, y muchos países que tienen capacidades militares inferiores en el sentido tradicional buscan usar la información para dividir y preocupar a sus adversarios. En Rusia, por ejemplo, influir en la opinión pública mediante la propaganda e inflamar las tensiones locales forma parte de su doctrina bélica y es algo que constantemente practican con aquellos a quienes perciben como sus adversarios. Las redes sociales cambiaron del todo el juego de los operativos de información. Ahora es más fácil que nunca mover la información rápidamente y hacerse pasar por otras personas, dando la impresión de que el público está enojado o dividido.

BUENO — lo que debe hacer

1. **Recuerde**: los operativos de información son un problema de comunicaciones, no uno técnico. Los adversarios pueden hacer que sus operativos sean más potentes robándole sus datos, pero una vez que la información está afuera en el entorno necesitará una estrategia de comunicaciones para manejarla. Piense por adelantado cómo manejar las noticias falsas o sesgadas: ¿las ignorará? ¿la reenviará por Twitter y reforzará que son falsas? ¿Cómo tomará esta decisión? Estas son algunas de las decisiones más difíciles que cualquier

campaña debe tomar, pero lo más importante es reflexionar con anticipación con su equipo acerca de estas interrogantes para que usted y su equipo tengan unos lineamientos sobre cómo responder, si deciden responder.

2. **Sepa qué está sucediendo**. Aliente a los activistas a que compartan las publicaciones, páginas o notas periodísticas a las que encuentren sospechosas. Si así lo desea puede nombrar a algunos pasantes o voluntarios para que se concentren específicamente en esto y hagan búsquedas para investigar qué contenidos hay allá afuera.. Un reto presente es que resulta imposible ver todo lo que los votantes podrían estar recibiendo en Facebook. Esta plataforma ha hecho que resulte más difícil publicar avisos políticos y ha incrementado el personal con que monitorear el contenido de las noticias, pero usted no puede revisar todo su contenido. La mejor forma de resolver esto hoy es encargándoselo a un equipo de voluntarios, que representen distintas geografías y grupos demográficos de su estado/distrito, para que así pueda captar la mayor información posible.

3. **Establezca contacto con plataformas de redes sociales claves y notifíquelas si encuentra información falsa o engañosa**. La mayoría de las plataformas de redes sociales ahora retiran el contenido "falso" o engañoso y los perfiles de impostores. Solicite a su comité de campaña o partido estatal (state party) relevantes el mejor contacto en las plataformas de las redes sociales y establezca un contacto al inicio de la campaña, para que así pueda contactarles rápidamente en caso de que algo salga mal.

    a. Facebook

    b. Twitter

    c. Google/Youtube

4. **Monitoree páginas impostoras**. Hasta la fecha no hay informes públicos de impostores que hayan intentado robar dinero o datos de activistas a través de páginas web falsas, pero es un vector de ataque tan fácil que deberá mantenerse alerta. Asegúrese de comprar toda dirección de Internet que pueda querer usar (pues podría ser usada contra usted). Si lo desea puede contratar un servicio de manejo de reputación que monitoree la web por usted. Algunos hacen esto por un precio bastante económico.

5. **Protéjase de un ataque de denegación de servicio distribuido (conocido como DDoS).** Un ataque de DDoS es cuando un adversario toma control de muchas de máquinas y las usa para que todas hagan "ping" a su página web a la vez, lo que hará que esta quede inactiva. En esta guía nos concentramos sobre todo en cómo mantener a la gente fuera de los datos de su campaña, pero en el caso de un DDoS se busca mantener su página abierta y disponible todo el tiempo para donantes y activistas. El DDoS aún no es una amenaza común en las campañas, pero se le podría emplear para bloquear su recaudación de fondos o simplemente causar una perturbación realmente frustrante a su campaña. Hay dos herramientas gratuitas que puede usar para proteger su página, Google Shield y Cloudflare.

¿Piensa usted en algunas formas de mejorar este manual?

¿Conoce nuevas tecnologías o vulnerabilidades a las que debiéramos responder?

Queremos recibir sus sugerencias.

Por favor comparta sus ideas, historias y comentarios en Twitter @d3p con el hashtag #CyberPlaybook, o escríbanos a connect@d3p.org para que así podamos seguir mejorando este recurso a medida que el entorno digital vaya cambiando.

El Proyecto Defendiendo la Democracia Digital
Centro de Ciencias y Asuntos Internacionales Belfer
Facultad Kennedy de Harvard
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P