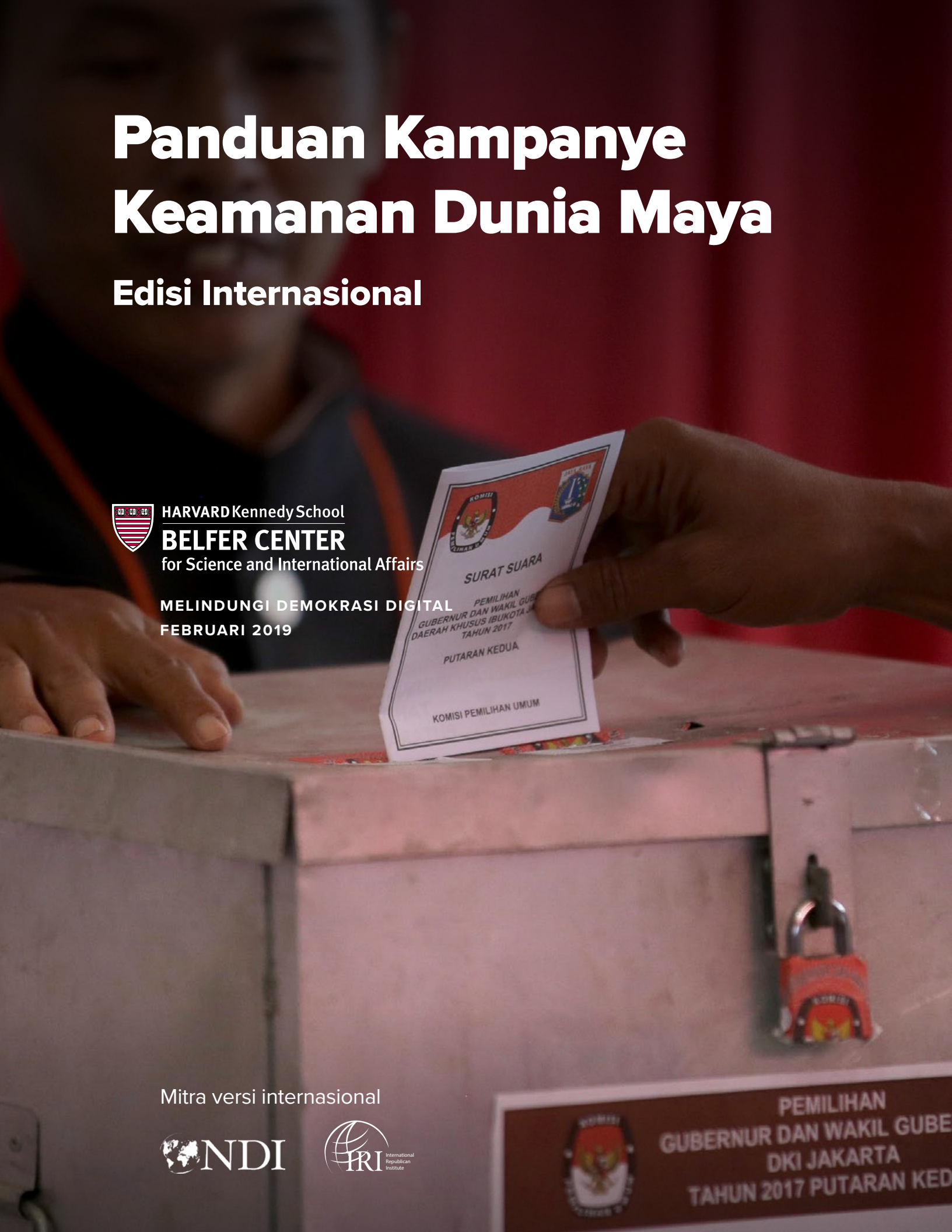
Panduan Kampanye Keamanan Dunia Maya

Edisi Internasional



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

MELINDUNGI DEMOKRASI DIGITAL
FEBRUARI 2019

Mitra versi internasional

NDI IRI International Republican Institute

Defending Digital Democracy Project
Melindungi Demokrasi Digital
Pusat Belfer untuk Sains dan Hubungan Internasional
Sekolah Pemerintahan John F. Kennedy

79 JFK Street
Cambridge, MA 02138
www.belfercenter.org/D3P

Mitra versi internasional:

Institut Demokrasi Nasional
www.ndi.org

Institut Internasional Republik
www.iri.org

Desain dan tata letak—Andrew Facini

Foto sampul: Seorang pria memberikan suaranya saat pemilihan lokal di Jakarta, Indonesia, Rabu, 19 April 2017. (AP Photo/Dita Alangkara)

Last updated 2019-02-19

Panduan Kampanye Keamanan Dunia Maya

Edisi Internasional

Daftar Isi

Selamat Datang

Orang bergabung dengan kampanye karena berbagai alasan: memilih pemimpin yang mereka percaya, memajukan agenda yang diusungnya, membersihkan pemerintah, atau mengalami kesibukan dan keseruan terlibat dalam kehidupan kampanye. Ini adalah beberapa alasan kita terlibat di ranah politik. Kami tentu tidak bergabung dalam kampanye karena kami ingin menjadi ahli mengenai dunia maya, dan kami duga anda pun sama.

Sayangnya, ancaman keamanan semakin meningkat dan mampu menghancurkan upaya kampanye Anda. Kami datang dari dunia kampanye dan mendukung proses demokrasi internasional, dan melihat dengan mata kepala kami sendiri ketika peretasan, pemberian informasi yang salah dan pencopotan laman (website) dapat memengaruhi jalannya pemilihan umum—dan haluan suatu negara.

D3P merupakan tim bipartisan keamanan dunia maya dan para ahli kebijakan dari sektor publik dan swasta, maupun ahli dengan pengalaman mendalam dalam kampanye politik. Kami bermitra dengan *International Republican Institute* (IRI) dan *National Democratic Institute* (NDI) agar dapat lebih memahami ranah pemilihan umum internasional dan bagaimana memikirkan dan melindungi diri dari risiko digital.

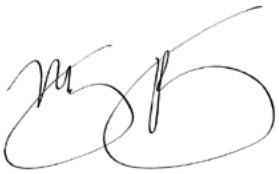
Kita datang dari partai politik yang berbeda-beda, dan seringkali tidak sependapat dalam hal kebijakan publik, namun satu hal yang memersatukan kita adalah kepercayaan bahwa para pemilih harus memilih dalam pemilu kita dan tidak boleh ada pihak lain lagi. Gaya hidup dan cara kerja kita yang semakin terdigitalisasi menawarkan berbagai cara baru bagi para lawan untuk memengaruhi kampanye dan pemilihan umum. Meskipun anda tak perlu menjadi ahli di dunia maya dalam menjalankan kampanye yang berhasil, anda punya kewajiban untuk melindungi kandidat dan organisasi anda dari musuh-musuh di ruang digital. Itulah mengapa sebuah proyek dari Harvard Kennedy School's Belfer Center for Science and International Affairs "Defending Digital Democracy" membuat **Cybersecurity Campaign Playbook** [PDF] ini.

National Democratic Institute, International Republican Institute dan banyak pejabat terpilih serta profesional di bidang kampanye bekerjasama dengan Proyek Defending Digital Democracy dalam mengadaptasi buku panduan itu untuk dapat digunakan oleh konteks internasional yang lebih luas.

Informasi yang dikumpulkan dan dirakit di sini dapat digunakan oleh kampanye apapun yang dilakukan oleh partai/pihak manapun. Buku ini dirancang agar dapat memberikan informasi yang sederhana, dapat dilaksanakan sehingga informasi kampanye anda lebih aman dari serangan-serangan lawan terhadap organisasi anda—dan demokrasi di negara anda. Dan utamanya, kami berharap sumber informasi ini memungkinkan anda meluangkan waktu untuk melakukan hal yang sudah berikan komitmennya—kampanye.

Semoga sukses!

Robby Mook
Hillary Clinton 2016 Campaign Manager.



Matt Rhoades
Mitt Romney 2012 Campaign Manager.

P.S. — Apakah Anda punya ide untuk membuat Playbook ini lebih baik? Apakah ada teknologi baru atau hal-hal sensitif lain yang harus kami tangani? Kami ingin anda memberikan umpan balik anda. Mohon dapat berbagi gagasan, cerita dan komentar anda di Twitter @d3p dengan memberikan tagar #CyberPlaybook atau kirimkan surat elektronik ke connect@d3p.org sehingga kami dapat memperbaiki sumber informasi ini seiring dengan perubahan lingkungan digital di dunia ini.

Penulis dan Kontributor

Proyek ini dapat terwujud karena kerja keras dari sejumlah orang yang telah sukarela meluangkan waktunya.

Terima kasih khususnya untuk **Debora Plunkett** untuk memimpin proyek dan **Harrison Monsky** untuk menulis dokumennya. Kami juga ingin menyampaikan rasa terima kasih mendalam kepada orang-orang di bawah ini yang telah meluangkan waktunya untuk mengulas draf dan memberikan masukan-masukannya.

DEFENDING DIGITAL DEMOCRACY LEADERSHIP

Eric Rosenbach, Co-Director, Belfer Center

Robby Mook, Belfer Center Fellow

Matt Rhoades, Belfer Center Fellow

AUTHORS AND CONTRIBUTORS

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**

BELFER CENTER WEB & DESIGN TEAM

Andrew Facini, Publications and Design Coordinator, Belfer Center

Pendekatan *Playbook* ini

Playbook Kampanye Keamanan Dunia Maya Internasional ini ditulis oleh banyak pihak dan tim ahli internasional dalam bidang keamanan dunia maya, politik dan hukum sehingga dapat memberikan cara-cara yang sederhana dan dapat dilakukan dalam meredam pertumbuhan ancaman dunia maya.

Serangan-serangan di dunia maya tak pandang bulu. Semua kampanye di seluruh tataran—bukan hanya kampanye nasional tingkat tinggi—pernah mengalami peretasan. Anda harus berasumsi anda adalah target/sasaran. Meskipun rekomendasi-rekomendasi di playbook ini dapat berlaku secara universal, namun buku ini diutamakan untuk kampanye yang tidak memiliki sumberdaya cukup dalam mempekerjakan staff keamanan dunia maya yang memadai. Kami menawarkan dasar yang kuat untuk strategi mitigasi risiko keamanan di dunia maya sehingga mereka yang tidak memiliki latar belakang pelatihan teknis dapat melaksanakannya (meskipun ada beberapa hal yang tetap membutuhkan profesional di bidang teknologi informasi).

Semua rekomendasi di sini sifatnya sangat mendasar, bukan referensi/rujukan komprehensif untuk mencapai tingkat keamanan setinggi mungkin. Kami sarankan semua kampanye untuk sedapat mungkin memastikan masukan profesional dari profesional di bidang teknologi informasi dan keamanan dunia maya yang berpengalaman dan terpercaya.

Pengantar

Kandidat dan kampanye menghadapi banyak sekali tantangan. Ada acara yang harus mereka selenggarakan, merekrut sukarelawan, mengelola demonstrasi publik, menggalang dana, menghubungi para pemilih, dan permintaan yang tiada henti dari siklus media modern. Setiap staf harus mengantisipasi hal-hal kejutan yang kurang menyenangkan misalnya hal-hal yang memalukan atau serangan iklan yang tiba-tiba. Serangan di dunia maya, kampanye informasi yang sesat, serta penyensoran internet masuk ke dalam daftar itu juga.

Karena kampanye saat ini semakin sering dijalankan secara digital, para musuh menemukan peluang-peluang baru untuk ikut campur, mengganggu dan mencuri. Pada tahun 2008, para peretas

dari Tiongkok menyusup ke dalam kampanye Obama dan McCain, kemudian mencuri sejumlah besar informasi dari keduanya. Pada tahun 2016, media sosial di Uganda harus dibungkam saat pemilihan umum. Pada tahun 2016, operasi maya dipercaya telah disponsori oleh pemerintah Rusia untuk mencuri dan membocorkan puluhan ribu surat elektronik dan dokumen dari staf kampanye Partai Demokrat AS, memberikan informasi-informasi yang mengganggu kampanye. Pada tahun 2017 partai-partai politik di Kenya menghadapi serbuan kampanye informasi sesat dan beberapa partai politik Serbia yang besar pun terpaksa membuat laman Facebook mereka luring (offline).

Konsekuensi pelanggaran yang dilakukan di dunia maya bisa sangat besar sekali. Berita tentang pelanggaran itu sendiri, dibumbui dengan pengeluaran informasi yang dicuri secara sedikit demi sedikit dapat melencengkan pesan kandidat selama berbulan-bulan. Para penyerang yang memenuhi laman (website) dapat memutus komunikasi anda dengan para pendukung anda atau berujung pada hilangnya donasi pada saat-saat penting. Pencurian donor personal atau data pemilih dapat mengakibatkan timbulnya tanggungjawab hukum, membuat para pendukung rentan mengalami pelecehan dan donor menjadi enggan berkontribusi pada kampanye anda. Serangan yang merusak yang ditujukan kepada komputer para staf atau server kampanye yang penting dapat memperlamban operasional kampanye selama berhari-hari atau bahkan berminggu-minggu. Membersihkan kekacauan yang ditimbulkan akan mengalihkan sumberdaya yang berharga pada masa-masa kompetisi yang sedang tinggi-tingginya, baik kompetisi untuk menjadi presiden, parlemen ataupun dewan perwakilan di tingkat kota.

Di masa yang akan datang, ancaman di dunia maya akan tetap menjadi bagian dari proses kampanye kita. Sebagai garda terdepan demokrasi, staf kampanye harus mengetahui risiko serangan, mengembangkan strategi untuk mengurangi risiko itu sedapat mungkin, dan menerapkan strategi tanggap risiko untuk saat itu ketika hal terburuk terjadi. Meskipun tidak ada satupun kampanye yang dapat mencapai keamanan sempurna, melakukan beberapa langkah sederhana dapat membuat pelaku jahat sulit melakukan niatnya. Ironisnya, para pemain yang tercanggih seringkali memilih metode penyerangan yang tidak terlalu canggih, memangsa orang dan organisasi yang abai terhadap protokol keamanan dasar. Ini adalah alasan utama mengapa kami membuat versi internasional dari Playbook Kampanye Keamanan Di Dunia Maya.

Dalam kampanye-kampanye di masa sekarang, keamanan dunia maya menjadi tanggungjawab semua pihak. Kesalahan manusia seringkali menjadi akar penyebab serangan di dunia maya yang mendapatkan perhatian publik, dan menjadi pilihan kandidat dan para pemimpin kampanye untuk memasukkan kesadaran akan keamanan ke dalam budaya organisasi. Keputusan yang

manusia buat sama pentingnya dengan piranti lunak yang mereka gunakan. Di masa yang akan datang, kampanye-kampanye terbaik akan punya standard yang jelas dalam hal kerja keras, pesan yang akan digaungkan, setia pada tim—dan mengikuti protokol keamanan yang baik.

Sebelum kami sampai pada rekomendasi, mari kita coba identifikasi masalah sesungguhnya:

- **Lingkungan tempat kampanye anda dijalankan**;
- **Ancaman yang mungkin anda hadapi; dan**
- **Pentingnya manajemen risiko dunia maya**.

Lingkungan Kampanye yang Rentan

Kampanye-kampanye yang dilakukan pada masa sekarang bisa menjadi sasaran empuk. Seringkali sifatnya sementara dan tidak berlangsung lama. Kampanye-kampanye ini tidak punya waktu maupun sumber dana untuk mengembangkan strategi keamanan jangka panjang yang teruji secraa keamanan. Sejumlah besar staf baru dapat dengan cepat memahami tanpa perlu melalui pelatihan yang lama. Mereka dapat membawa piranti keras mereka sendiri dari rumah—dan malware pun mengintai! Banyak kontributor kampanye hidup dan bekerja ratusan kilometer jauhnya dari kantor pusat. Segala sesuatu bergerak dengan cepat, banyak yang dipertaruhkan, dan banyak yang merasa tidak punya waktu untuk memedulikan mengenai keamanan dunia maya. Ada banyak sekali celah untuk kesalahan di sini.

Pada saat yang bersamaan, kampanye-kampanye banyak yang semakin bergantung pada informasi-informasi mengenai pemilih, donor dan pendapat masyarakat. Mereka juga menyimpan dokumen-dokumen yang sensitif, misalnya penelitian oposisi, studi mengenai kerentanan, daftar pendukung, dokumen pemeriksaan personil, makalah kebijakan draft awal, dan surat elektronik. Risiko serangan pun semakin meningkat demikian pula konsekuensinya.

BAHAYANYA SERANGAN

Bayangkan ini: Sebulan sebelum hari pemilihan umum, dan persaingan pun makin ketat. Anda tiba di kantor pusat lebih awal, mengambil secangkir teh atau kopi, menuju meja kerja anda dan masuk ke dalam komputer anda. Tiba-tiba muncul layar hitam, kemudian gambar kartun kandidat anda dalam posisi yang menjijikkan muncul diikuti dengan sebuah pesan. Hard-drive anda terhapus semua. Setiap informasi digital yang anda kumpulkan—memo, daftar sasaran, *balance sheet*—semua hilang. Dalam pesan itu terbaca untuk mendapatkannya kembali anda akan butuh jutaan rupiah—atau penolakan terhadap posisi kebijakan utama.

Kelompok yang tak dikenal meretas komputer anda beberapa bulan yang lalu dan diam-diam mencuri surat elektronik, memo strategi, alamat para donor, dan nomor jaminan sosial serta KTP para staf. Kelompok ini menghabiskan berminggu-minggu menyisir banyaknya informasi yang ada dan mendistribusikan beberapa informasi penting di media sosial dan melalui laman yang mudah digunakan yang sengaja dibuat untuk menyebarluaskan informasi penting tersebut. Isi laman itu utamanya adalah sejumlah besar 'penelitian mandiri' yang dilakukan terhadap kandidat anda. Untuk saat ini, laman kampanye sudah dinonaktifkan, akun media sosial pun ditangguhkan untuk membersihkan gambar-gambar tak senonoh, dan tidak ada satupun komputer yang dapat berfungsi yang terlihat.

Ancaman-ancaman yang dihadapi Kampanye

Sayangnya, bagi kampanye dan demokrasi di seluruh dunia, para musuh yang ada di dalam maupun luar negeri mengira melukai atau membantu kandidat tertentu akan memajukan kepentingan mereka, dalam hal ini menimbulkan kekacauan dan kebingungan di kalangan para pemilih, atau menghukum pejabat yang bersuara menentangnya. Mungkin ini terdengar seperti fiksi yang mencekam, namun kenyataannya jasa intelejen yang canggih, cybercriminal atau hacktivist dengan dendam kesumat terhadap kandidat dapat memutuskan siapa yang akan menjadi sasarannya, anda atau orang lain dalam kampanye anda. Ini adalah hal-hal yang harus disadari oleh para manajer dan staf yang menangani ancaman.

Karena komunikasi kampanye yang memiliki informasi sesat dan yang dimanipulasi menjadi sumber informasi untuk menipu dan menyesatkan banyak warga negara di dunia, informasi yang dicuri, dimanipulasi dan dibocorkan dapat mendatangkan konsekuensi nyata terhadap pemilihan umum anda. Mekanisme yang sudah anda miliki untuk melindungi data anda dan menjaga jalur komunikasi sekarang menjadi lebih penting dari sebelumnya.

SIAPA YANG MERETAS?

Kampanye menghadapi ancaman informasi dan keamanan di dunia maya dari berbagai jenis pelaku. Peretas tunggal “black hat” dan cybercriminals telah berusaha menghancurkan kampanye karena alasan pribadi, ingin dikenal, atau hanya sekadar ingin tahu apakah mereka bisa melakukannya. Negara-negara menjadi sumber ancaman yang paling menjadi membahayakn. Kelompok spionase Rusia yang dikenal dengan “Fancy Bear” (APT 28) dan “Cozy Bear” (APT 29) dituduh melakukan kegiatan peretasan kampanye pada tahun 2016 di AS. Negara Tiongkok banyak fokus pada pengumpulan informasi. Ditengarai mereka telah aktif pada kampanye presiden tahun 2008 dan 2012 di AS, namun tidak ada bukti mereka mengeluarkan materi-materi yang mereka curi. Korea Utara terkenal melakukan balas dendam terhadap Sony Pictures Entertainment karena memproduksi film “The Interview” dengan mencuri dan mengeluarkan surat elektronik perusahaan dan menghapus sistem mereka. Di beberapa negara kampanye-kampanye oposisi dapat menghadapi ancaman dari pemerintah mereka juga. Semakin menguatnya ketegangan internasional—terutama di sekitar penyelenggaraan pemilihan umum yang berisiko tinggi—dapat menimbulkan serangan-serangan di masa yang akan datang.

Mengelola Risiko di Dunia Maya

Risiko dibagi menjadi tiga bagian. Pertama, *kerentanan*: kelemahan dalam kampanye anda menjadikan informasi rentan pencurian, perubahan atau pengrusakan. Kerentanan dapat berasal dari piranti keras, piranti lunak, proses, dan tingkat kewaspadaan staf anda. Kemudian *ancaman* sesungguhnya: negara, hacktivist, dan kelompok-kelompok non-negara lainnya yang memiliki kemampuan untuk mengeksploitasi kerentanan-kerentanan tersebut. Risiko ada ketika kerentanan dan ancaman bertemu. Yang terakhir adalah *konsekuensi*—dampak yang terjadi ketika pelaku jahat menggunakan risiko yang tidak termitigasi.

Tidak ada yang dapat Anda atau kampenye anda lakukan untuk mencegah ancaman—karena mereka adalah hasil dari kekuatan geopolitik, ekonomi dan sosial yang lebih besar lagi. Yang dapat anda lakukan adalah mengurangi kemungkinan musuh-musuh anda berhasil menyerang anda dengan mengurangi kerentanan anda. Dengan berkurangnya kerentanan maka risiko pun berkurang—menjadi keputusan anda untuk menentukan mana yang perlu dikurangi. Misalnya, anda bisa memutuskan hal terburuk yang dapat dilakukan oleh seorang peretas adalah mencuri laporan penelitian mandiri kandidat anda, sehingga anda akan meluangkan sumber daya ekstra untuk mengamankan penyimpanan data berbasis teknologi cloud, membutuhkan kata kunci yang panjang dan akses terbatas untuk segelintir orang saja. Anda juga dapat memutuskan membuat dokumen lain mengenai kampanye tersedia secara luas dan tidak terlalu aman, karena banyak yang membutuhkannya untuk menjalankan pekerjaan mereka dan bila bocor kerugian maupun kerusakannya tidak terlalu mengkhawatirkan. Ingatlah bahwa langkah-langkah yang dilakukan untuk mengamankan data mereka dan menanggapi insiden di dunia maya juga harus terlindungi dengan perlindungan data dan hukum privasi yang ada di dunia, misalnya *General Data Protection Regulation* (GDPR) di Eropa.

Ada beberapa aspek teknis untuk memitigasi risiko dan kami juga memiliki rekomendasi teknis dalam playbook ini, namun yang terpenting adalah pendekatan holistik yang anda terapkan. Sebagai pemimpin kampanye, hal terpenting yang harus anda lakukan adalah membuat pilihan-pilihan mendasar, misalnya siapa yang dapat mengakses informasi, informasi apa yang disimpan atau disebar, berapa waktu yang dibutuhkan untuk pelatihan dan perilaku anda sebagai teladan. Sebagai profesional di bidang kampanye, manajemen risiko menjadi tanggung-jawab anda—baik secara teknis maupun SDM. Menjadi keputusan anda data dan sistem mana yang paling berharga dan sumberdaya yang mana yang anda alokasikan untuk melindunginya.

Mengamankan Kampanye Anda

Rekomendasi Keamanan Kami diatur menurut tiga prinsip berikut:

1. Persiapkan:

Keberhasilan dari hampir semua rekomendasi Playbook ini bergantung pada pimpinan kampanye yang menciptakan budaya kewaspadaan keamanan yang mengurangi rantai terlemah. Artinya kita harus membuat aturan dasar yang jelas yang ditegakkan dari tampuk pimpinan teratas hingga terendah dan juga diterima dari bawah ke atas.

2. Perlindungan:

Perlindungan penting. Ketika anda tahu anda memiliki masalah keamanan, itu sudah terlambat. Membangun pertahanan terkuat yang dapat anda sanggupi secara waktu maupun biaya menjadi kunci dalam mengurangi risiko. Keamanan internet dan data bekerja dengan sangat baik ketika dilakukan secara berlapis: tidak ada teknologi atau produk tunggal yang bisa dijalankan dengan baik. beberapa tindakan dasar yang digabungkan satu sama lain akan membuat arsitektur digital kampanye sulit dilanggar dan lebih kuat bila mengalami gangguan, dan pada akhirnya menghemat waktu kampanye dan uang di masa yang akan depan.

3. Gigih:

Kampanye kini menghadapi banyak musuh yang memiliki sumberdaya dan keahlian yang sangat tinggi; bahkan budaya yang paling awas sekalipun dan infrastruktur yang paling kuat tidak akan dapat mencegah pelanggaran keamanan. Kampanye perlu mengembangkan rencana sebelumnya untuk menangani pelanggaran bila hal itu terjadi.

Beberapa kampanye mungkin punya waktu dan uang untuk menangani keamanan dunia maya dibandingkan dengan kampanye lainnya. Itulah mengapa rekomendasi kami menawarkan dua tingkat perlindungan "baik" dan "sangat baik." Tingkat "baik" merupakan semua hal yang harus dilakukan kampanye sehingga bisa mendapatkan tingkat keamanan minimum. Anda harus berupaya untuk melakukan lebih baik lagi, seiring dengan waktu, uang dan SDM yang anda miliki, itulah mengapa kami merekomendasikan untuk menggunakan tingkatan "sangat baik" sedapat mungkin. Bila anda punya sumber daya untuk mendapatkan dukungan teknologi informasi yang memiliki reputasi baik dan terlatih, maka ini adalah pengeluaran yang patut dan sepadan. Ancaman seringkali berubah dan layanan TI profesional akan dapat membawa anda ke posisi yang melampaui apa yang disediakan oleh playbook ini dan anda menjadi semakin paham dengan ancaman terkini dan mendapatkan solusi atas situasi anda.

Manajemen

Para manajer Kampanye harus bertanggungjawab untuk strategi keamanan dunia maya, namun sebagian besar akan mendelegasikan pengembangan dan pengawasannya kepada wakil direktur atau direktur operasional. Penting bagi keamanan dunia maya untuk diintegrasikan ke dalam SDM dan Teknologi informasi, karena memilih SDM yang tepat, penyediaan piranti keras, dan pengendalian ijin akan sangat penting bagi strategi anda. Banyak kampanye kecil yang bergantung pada bantuan sukarela untuk TI dan keamanan dunia maya. Anda dapat menggunakan playbook ini dalam memandu diskusi anda dengan bantuan sukarelawan. Kuncinya adalah secara cermat dan teliti memeriksa latar belakang sukarelawan yang membantu anda dan dengan hati-hati mengendalikan akses sehingga bantuan dari sukarelawan pun tidak akan menimbulkan kerentanan baru. Anda harus memastikan staf kampanye melakukan pengawasan terhadap kerja TI dan mengendalikan ijin untuk mengakses sistem-sistem yang berbeda.

Kapan memulai

Apapun model bantuan yang anda miliki, *keamanan dunia maya harus dimulai sejak hari pertama*. Setelah itu "lima daftar periksa teratas" dari tindakan-tindakan yang sangat penting. Pastikan semua ini ada sejak awal, bahkan ketika hanya ada satu atau dua orang staf, kemudian jalankan rekomendasi-rekomendasi "baik" lainnya sesegera mungkin. Bila tindakan-tindakan ini belum menjadi bagian dari rencana digital pertama anda, jangan khawatir. Belum terlambat untuk mengadopsi tindakan-tindakan pengamanan dan melindungi apapun yang sudah anda lakukan sekarang.

Biaya

Banyak yang kami rekomendasikan di sini tidak berbayar atau bilapun berbayar sangat murah. Bahkan semua yang ada di dalam daftar lima tindakan teratas yang kami rekomendasikan tidak membutuhkan biaya, kecuali mendapatkan platform penyimpanan berbasis teknologi cloud, yang sebetulnya hanya beberapa dollar saja per bulan per pegawai. Kampanye dengan target tinggi harus menganggarkan sumberdaya yang cukup untuk piranti keras dan piranti lunak dalam menjalankan strategi yang bertanggungjawab, namun ini hanya sedikit dari jutaan dollar anggaran kampanye. Kampanye-kampanye kecil akan dapat menjalankan rekomendasi-rekomendasi di sini dengan biaya hanya ratusan dollar hingga beberapa ribu dollar saja, bergantung pada banyak staf atau sukarelawan yang bekerja di kampanye.

Setiap rujukan terhadap vendor dan produk memang untuk memberikan contoh solusi yang umum, namun bukan berarti kami mempromosikan produk tersebut. Bila muncul tantangan

dalam menggunakan produk atau layanan, kami sarankan anda hubungi vendor secara langsung yang dapat memberikan bantuan teknis di tataran pengguna. Dalam memilih produk dan layanan, kami sarankan setiap kampanye berkonsultasi dengan ahli bidang keamanan dunia maya atau melakukan riset mandiri untuk menemukan produk yang sesuai dengan kebutuhan mereka.

Lima Daftar Periksa Terpenting

1. Bangun budaya sadar keamanan informasi:

Anda harus menanggap keamanan dunia maya sebagai sesuatu yang sangat serius. Bertanggungjawablah dalam mengurangi risiko, melatih staf dan sukarelawan Anda, dan memberikan contoh. Kesalahan manusia merupakan penyebab utama pelanggaran.

2. Gunakan *cloud*:

layanan penyimpanan data berbasis cloud yang besar dan komersial akan jauh lebih aman daripada apapun yang anda lakukan dengan sumberdaya yang terbatas. Pertimbangkanlah menggunakan piranti lunah berbasis cloud seperti Gsuite atau Microsoft365 yang akan memberikan fungsi kantor dasar dan tempat aman menyimpan informasi (lihat “Apa itu Cloud” pada halaman. 16).

3. Gunakan otentikasi dua faktor (2FA) dan kata kunci yang kuat:

Persyaratkan otentikasi dua faktor (2FA) agar dapat menambahkan lapisan perlindungan ke dua bagi semua akun penting, termasuk office suite anda, surat elektronik atau layanan penyimpanan, dan akun media sosial. Gunakan aplikasi mobile atau kunci fisik untuk faktor kedua anda, bukan pesan teks. Untuk kata kunci, buatlah SESUATUYANGSEPANJANGINI, bukan sependek l17i . Berbeda dengan yang dipercaya banyak pihak, kata acak yang panjang tanpa simbol lebih sulit untuk diterka dibandingkan dengan kata yang pendek dengan B417nyAk_$imBoL. Jangan pernah mengulang kata kunci; manajer kata kunci dapat membantu dalam hal ini, dengan memberikan kesempatan anda untuk secara acak membuat kata kunci yang kuat dan mengaudit kata kunci anda untuk menidentifikasi kata kunci yang sudah pernah digunakan sebelumnya.

4. Gunakan pesan yang terenkripsi untuk perbincangan dan material yang sensitif:

Dengan menggunakan alat pengirim pesan yang terenkripsi seperti Signal atau Wickr untuk pesan-pesan dan dokumen yang sensitif artinya para musuh tidak akan bisa mengambilnya bila mereka meretas surat elektronik anda. Enkripsi mengacak data, dapat dengan signifikan mengurangi kemungkinan orang lain membaca pesan anda bahkan ketika mereka melakukan intersepsi terhadap data.

5. Rencanakan dan Siapkan:

Buat rencana bila keamanan anda terancam. Ketahui siapa yang harus anda hubungi ketika ada permasalahan teknis, memahami kewajiban hukum anda, dan bersiaplah untuk mengkomunikasikan permasalahan secara internal dan eksternal secepat dan seefektif mungkin.

Langkah-langkah untuk Mengamankan Kampanye anda

Langkah 1: Unsur Manusia

Keamanan di dunia maya secara mendasar adalah permasalahan manusia, bukan masalah teknis. Solusi teknis terbaik di dunia ini tak akan berdampak apapun bila tidak dijalankan dengan tepat, atau ketika tidak diperbarui seiring dengan kemajuan dan perubahan teknologi. Praktik keamanan dunia maya yang berhasil bergantung pada upaya untuk menciptakan budaya keamanan.

BAIK — Apa Yang Perlu Anda lakukan

1. Buatlah budaya keamanan informasi yang kuat sebagai standard untuk memenangkan kampanya. Sama halnya ketika staf kampanye diinstruksikan untuk tidak melanggar undang-undang keuangan kampanye, para pegawai juga harus tahu bagaimana caranya menghindari menekan tautan atau membuka lampiran di surat elektronik dari pengirim yang tidak dikenalnya.

    a. **Onboarding**: berikan pelatihan keamanan informasi dasar ketika anda mempekerjakan staf baru. Anda dapat membagikan selebaran untuk Staf saat pelatihan.

    b. **Pelatihan**: Jadikan keamanan bagian dari pelatihan staf anda, misalnya acara staf senior atau pelatihan pra pemilu untuk mendapatkan suara (get-out-the-vote, GOTV). Berikan pelatihan tambahan bagi mereka yang menjalankan peran sensitif, misalnya kandidat, staf bidang media, staf senior, dan siapapun dalam administrator sistem yang memiliki keistimewaan di jaringan anda. Para manajer harus mensyaratkan semua orang-orang yang penting dalam kampanye—termasuk kandidat—diperiksa keamanannya oleh siapapun yang mengelola teknologi informasi (yang mungkin manajer itu sendiri). Jangan ragu atau setengah-setengah soal keamanan kandidat dan VIP lainnya!

    c. **Jadilah teladan**: staf kampanye senior dan kandidat harus mengambil peran pemimpin yang nyata, mengadvokasi keamanan dunia maya saat pelatihan. Staf senior harus terus menerus memberikan penguatan tentang pentingnya keamanan dunia maya kepada para staf junior di pertemuan dan kapanpun diperlukan. Jangan hanya menggantungkan pada para ahli teknis dalam menjalankan pelatihan. Manajer kampanye atau direktur operasional dapat menjadi penyampai pesan yang kuat karena mereka dipandang tidak terlalu “teknis.”

2. Lakukan pemeriksaan latar belakang yang teliti terhadap para staf, sukarela, dan pekerja magang—siapapun yang memohon akses informasi kampanye—untuk menghindari memberikan kepercayaan kepada orang yang ingin mencuri data atau menyabotase sistem anda.

    a. Tentukan definisi informasi sensitif dan aturan penggunaannya. Misalnya, anda bisa memilih untuk mengelompokkan semua pengambilan suara, materi penelitian, memo strategi dan surel terkait sebagai “sensitif”.

    b. Larang pengalihan informasi sensitif pada jalur komunikasi yang tidak dikelola dan diamankan kampanye. Anda dapat mensyaratkan agar semua informasi itu dialihkan melalui penyampaian pesan yang terenkripsi. (lihat Langkah 2).

3. Konfirmasi bahwa konsultan dan vendor yang dapat mengakses informasi sensitif memiliki surel dan penyimpanan data yang aman (lihat Langkah 2). Bila ragu, terapkan syarat vendor dan konsultan menggunakan akun dalam office suite yang berbasis cloud (lihat Langkah 2).

4. Kendalikan akses terhadap layanan daring yang penting, misalnya akun medsos kampanye resmi, untuk menghindari penggunaannya oleh individu yang tidak memiliki wewenang. Pastikan siapapun yang meninggalkan kampanye tidak dapat mengakses semua akun yang berhubungan dengan kampanye. Anda bisa dengan mudah melakukannya melalui alat pengendalian akun media sosial yang menjadi pintu masuk semua akun anda. Bila ada yang meninggalkan kampanye, anda harus dengan segera menghentikan aksesnya terhadap akun tersebut.

5. Beri informasi kepada para staf tentang ancaman phising. Pastikan mereka tahu caranya mengenali dan menghindari tautan yang mencurigakan dan menekankan pentingnya mengidentifikasi dan melaporkan serangan phishing potensial. Sebagai bagian dari budaya keamanan kampanye yang kuat, staf senior harus mengenali dan memberikan penghargaan kepada semua yang melaporkan perilaku yang mencurigakan pada sistem mereka atau mengakui telah menekan tautan yang memiliki potensi berbahaya.

6. Pahami lingkungan hukum anda. Di beberapa tempat, misalnya Uni Eropa, standard privasi mewajibkan beberapa persyaratan tertentu tentang data yang dikumpulkan oleh kampanye anda, terutama informasi yang dapat dengan mudah mengaitkannya dengan diri kita misalnya demografi atau data alamat.

Selebaran

» Bagi staf

» Bagi anggota keluarga

LEBIH BAIK — Ambil Langkah Berikutnya

7. Produk-produk piranti lunak seperti Phisme dan KnowBe4 dapat melatih staf anda dengan mengirimkan kepada mereka surel phising palsu. Hal ini menjadi cara yang teraman, cepat dan efektif untuk mempelajari siapa saja yang paling berisiko menekan tautan, sehingga anda bisa memberikan pelatihan ekstra kepada mereka. Banyak dari produk-produk ini juga menyaring beberapa upaya phising terhadap surel anda.

8. Bila anda punya sumberdayanya, rekrutlah profesional di bidang IT untuk membantu mengelola sistem kampanye Anda dan ahli keamanan IT yang membantu anda melindungi, memelihara, dan memantau infrastruktur digital kampanye anda. Dia bisa memberikan pelatihan keamanan rutin dan menguji SDM serta sistem, sembari memberikan solusi keamanan yang sesuai dengan kebutuhan.

9. Buatlah kontrak kerjasama dengan firma keamanan dunia maya untuk memberikan solusi keamanan, menilai seberapa jauh ketahanan anda, dan/atau memantau sistem bila ada pelanggaran. Ketahui firma mana yang akan anda hubungi bila ada pelanggaran dan perlu bantuan tanggap segera. Ini merupakan salah satu alternatif dari merekrut ahli keamanan IT purnawaktu. Lakukan riset dan pilihlah firma yang memiliki reputasi baik—tidak semua firma keamanan dunia maya memberikan tingkat layanan yang sama.

BEKERJA DENGAN PROFESIONAL DI BIDANG KEAMANAN

Bila Anda memutuskan bekerja dengan profesional di bidang keamanan, bagaimanakah anda akan mengevaluasi orang atau firma yang tepat? Baik melalui rekomendasi personal atau ulasan masyarakat yang positif, sangatlah penting anda menghindari bantuan/dukungan yang tidak efektif namun mahal. Ketika anda mewawancari profesional keamanan potensial, tanyakan bagaimana mereka menanggapi insiden keamanan masa lampau dan bagaimana mereka memungkinkan yang lain bekerja dengan lebih aman. Komite partai nasional anda atau profesional kampanye yang terpercaya dapat merekomendasikan anda beberapa pilihan. Ingatlah bahwa budaya memengaruhi keamanan dan bahkan rekomendasi terbaik sekalipun akan gagal bila tidak diikuti (dalam hal ini hanya mempekerjakan firma saja tidak menyelesaikan masalah anda).

Langkah 2: Komunikasi

Tidak semua metode komunikasi aman, sehingga sebaiknya anda harus lugas saat berkomunikasi. Kepemimpinan kampanye harus mengatur standard yang mendorong perbincangan langsung sedapat mungkin, dan hindari surel yang bertele-tele ataupun tidak penting. Apapun yang anda tulis di dalam surel dapat dipublikasikan di koran atau media sosial—mungkin setelah diubah secara sengaja. Apapun bentuknya, telepon, pesan singkat, atau email, produk dan layanan yang berbeda menawarkan tingkat perlindungan yang berbeda pula, jadi lakukan riset sebelum anda memilih sistem mana yang akan digunakan oleh kampanye anda.

BAIK — Apa Yang Perlu Anda lakukan

1. Gunakan sistem teraman untuk komunikasi.
    a. Gunakan layanan pengiriman pesan terenkripsi end-to-end misalnya Signal atau Wickr, terutama untuk pesan, berbagi dokumen dan telepon. Banyak kampanye mewajibkan informasi sensitif disampaikan melalui layanan pengiriman pesan terenkripsi, dan seringkali ini merupakan cara termudah bagi para staf kampanye untuk membiasakan diri menggunakan aplikasi-aplikasi ini dalam komunikasi rutin mereka (ini merupakan langkah cerdas terutama untuk individu yang memiliki risiko tinggi seperti kandidat). Signal dan Wickr mempublikasikan source code mereka untuk ditinjau dan memberikan fungsi yang mengurangi risiko, misalnya memberikan pilihan pada anda untuk menghapus pesan secara otomatis. Pastikan pesan-pesan anda tidak disinkronkan dengan komputer atau akun cloud yang tidak terenkripsi
    b. Matikan fitur ‘archiving’ dalam layanan pengiriman pesan, misalnya Google Chat dan Slack, sehingga percakapan lama tidak bisa dicuri nantinya. Untuk melakukannya anda harus menuju ke ‘settings’ dan menyesuaikan ‘retention policy’. Beberapa layanan meminta anda melakukannya untuk setiap percakapan. Kami sarankan untuk menyimpan percakapan satu minggu atau kurang.
2. komunikasi surel, pembuatan dokumen, percakapan, dan berbagi file yang aman misalnya GSuite atau Microsoft365. Misalnya, Gsuite termasuk Google Drive untuk berbagi file, Gmail untuk surel, Google Hangouts untuk percakapan, dan Google Docs untuk word processing, spreadsheets, dan presentasi. Microsoft365 menawarkan OneDrive/SharePoint untuk berbagi file, Outlook/Exchange untuk surel, Microsoft Teams untuk percakapan, dan Microsoft Office untuk word processing, spreadsheets, dan presentasi. Kecuali Anda mempekerjakan profesional yang sangat berpengalaman (dan mungkin sangat mahal), sistem berbasis cloud yang dikelola oleh firma besar akan lebih terlindungi dari server yang anda bangun dalam kampanye anda. Ada versi gratis dari produk ini, namun versi berbayarnya memberikan kemampuan administratif lebih untuk anda. Google juga menawarkan layanan gratis untuk melindungi organisasi dalam lingkungan yang penuh

ancaman, misalnya Outline, VPN yang dapat di-host secara mandiri; Project Shield, layanan untuk melindungi laman anda dari serangan yang melumpuhkan; dan Password Alert, yang memperingatkan anda bila anda memasukkan kata kunci Gmail anda di laman phising.

3. Hapus surel anda

    a. Nyalakan fitur Auto-delete dalam aplikasi surel untuk surel lama sehingga mengurangi jumlah surel yang mungkin dicuri. Dalam melakukan hal ini anda harus masuk dan mengubah "retention policy" ke periode yang lebih singkat pada tab "settings". Untuk memastikan surel anda tidak berada terlalu lama dalam folder "deleted items", atur pembersihan otomatis (auto-purge) setelah beberapa waktu. Kami sarankan menyimpan surel hanya untuk masa satu bulan atau kurang, kecuali memang disyaratkan secara hukum untuk menyimpannya dalam waktu yang lama. Mereka tidak akan bisa mencuri apa yang tidak anda punya.

4. Amankan akun personal anda

    a. Bisnis kampanye tidak boleh menggunakan akun pribadi. Namun, para musuh akan menyasar akun personal untuk peretasan, sehingga mintalah para staf anda menggunakan kata kunci yang kuat dan otentikasi dua faktor untuk akun pribadi mereka juga (ini dimasukkan dalam selebaran untuk para staf).

APAKAH CLOUD ITU?

"Layanan Cloud" memberikan pengaturan dan akses informasi yang disimpan jarak jauh di internet. Mereka menjalankan server di luar lokasi yang dikelola oleh perusahaan pihak ke tiga; termasuk layanan-layanan yang sudah anda ketahui sebelumnya, misalnya Gmail atau Dropbox. Ada baiknya anda menyimpan informasi dengan penyedia layanan cloud terpercaya dan bukan di komputer pribadi anda karena para penyedia layanan ini punya dana, sumberdaya teknis dan keahlian untuk membuat server mereka lebih aman daripada hard-drive laptop atau server kantor anda. Mereka juga punya banyak staf teknis yang bekerja untuk melawan serangan-serangan canggih terhadap jaringan mereka (dan juga data anda). Ini seperti perbedaan menyimpan uang di bawah kasur dan menyimpannya di tempat aman di bank. Menggunakan layanan cloud akan menambahkan pengaman terhadap hilangnya data bila alat individual hilang atau terganggu. Penyimpanan cloud merupakan salah satu fitur yang terdapat dalam layanan keamanan kantor yang menyeluruh seperti Gsuite dan Microsoft365. Layanan lain termasuk Dropbox atau Box. Penting untuk mengingat bahwa perusahaan-perusahaan internasional ini mungkin harus mengikuti permintaan penegakan hukum untuk memberikan riwayat kontak, surel, atau isi berkas. Sebagian perusahaan besar seperti yang disebutkan di sini punya kebijakan-kebijakan yang ketat mengenai kapan mereka akan mengikuti permintaan semacam itu.

BAGAIMANA BILA SAYA TIDAK PERCAYA PADA CLOUD?

Beberapa organisasi merasa tidak nyaman memercayakan informasi mereka kepada perusahaan pihak ke tiga. Bila anda bersikukuh mengelola infrastruktur teknologi anda sendiri, bersiaplah anda mungkin harus menghadapi kekuatan keamanan dari bangsa lain. Beberapa hal yang perlu dipertimbangkan:

- Anda bertanggungjawab untuk memahami, mengamankan dan memperbaiki semua aspek dalam sistem anda, termasuk sistem operasional, aplikasi server, piranti lunak, basis data dan teknologi koneksi.
- Anda harus memastikan koneksi ke platform utama anda dapat diandalkan dan tidak rentan mengalami manipulasi, penyensoran atau DDOS.
- Anda harus secara aktif memantau retasan dan ada yang bisa anda hubungi setiap saat 24 jam seminggu.
- Anda harus mengelola backup yang aman dan di luar lokasi.
- Bila anda berisiko mengalami serbuan secara fisik, informasi anda dapat dirampas.

APA ITU ENKRIPSI?

Enkripsi adalah cara untuk menyandikan informasi ketika informasi itu berjalan dari satu pengguna ke pengguna lain, atau ketika disimpan, sehingga tidak dapat dibaca dengan mudah oleh siapapun kecuali penerima yang sesungguhnya. Jadi seperti ini contohnya: seorang pengguna "mengacak" data ketika ia mengirimnya dan hanya penerima sesungguhnya yang punya kunci untuk mengurutkannya. Penggunaan enkripsi adalah langkah cerdas, terutama untuk informasi yang sensitif, karena bahkan bila lawan kita mencuri data tersebut, mereka mungkin tidak akan bisa membacanya. Sebagian besar aplikasi yang menggunakan enkripsi seperti Signal atau Wickr, membuat proses ini sangat mudah. Enkripsi end-to-end merupakan fitur penting dalam program komunikasi—artinya pesan anda bersifat rahasia dari telefon atau komputer anda sampai ke tujuan, dan tidak akan ada seorangpun—termasuk penyedia layanan—yang dapat membaca pesan itu. Bila mungkin gunakan enkripsi whole-disk di laptop anda; bila dicuri atau tertinggal di bis misalnya, tak akan ada seorang pun yang dapat membaca kontennya.

PENYENSORAN, SURVEILANS, DAN *INTERNET SHUTDOWNS*

Sayangnya di banyak tempat di dunia ada tren yang semakin meningkat yang berupaya untuk menggoyahkan internet sebagai ruang yang terbuka dan demokratis. Termasuk upaya membloking jalur-jalur komunikasi penting misalnya WhatsApp atau Twitter; menyensor laman publik; atau secara agresif mengintai warga negara yang mengunjungi properti daring anda dan apa yang staf anda lakukan secara daring. Dalam situasi terburuk, yang semakin mengkhawatirkan, suatu negara bahkan bisa memutus akses internet sama sekali.

Selalu punya rencana cadangan. Bila partai atau kampanye anda bergantung pada laman kampanye, pastikan laman Facebook anda memiliki informasi terpenting bila laman anda nanti diblok atau sensor. Bila WhatsApp merupakan jalur komunikasi utama, bersiaplah untuk menggunakan SMS atau sediakan pohon telefon cadangan dengan nomor semua orang di dalamnya. Bila pemantauan lalu lintas dunia maya atau kegiatan daring staf kampanye anda dapat mendatangkan masalah, pertimbangkan menggunakan alat-alat penghambat atau anonimisasi seperti Tor Browser[1], Psiphon[2] atau Outline[3] do-it-yourself VPN. Buatlah daftar nama jurnalis yang dapat anda hubungi dengan mudah, dan ketika terjadi perubahan besar dalam hal penyensoran atau internet shutdown, bantu mereka membuat cerita mengenai hal itu.

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

MENJAGA AGAR LAMAN ANDA TETAP DALAM JARINGAN (DARING)

Laman kampanye anda mungkin salah satu platform komunikasi publik terpenting yang anda punya, dan salah satu cara termudah bagi warga untuk menemukan anda. Hal ini membuat khadiran anda di dunia maya menjadi sasaran empuk para peretas jahat atau lawan yang amoral. Pertimbangkan untuk menggunakan hosting platform, seperti Wordpress.com, Wix, atau Google Pages dimana anda tidak bertanggungjawab menjadi administrator keamanan laman sendiri. Bila anda mau mengelola laman anda sendiri, pastikan anda memiliki keahliannya atau anda dapat mempekerjakan profesional untuk menjaga keamanannya dari peretasan.

Para penyerang making sering meluncurkan serangan-serangan “distributed denial of service” (DDOS) untuk menjadikan laman luring saat masa-masa kritis melalui permohonan bohongan bervolume besar. Content Distribution Network (CDN) dapat menyimpan cached copy laman Anda di server yang kuat di seluruh dunia, menjadikannya sulit untuk dihancurkan. Dua produk yang punya kemampuan untuk membantu dengan melindungi laman publik anda adalah Cloudflare dan Google’s Project Shield.

Langkah 3: Akses dan Pengelolaan Akun

Salah satu aspek yang paling sulit dari keamanan adalah menjaga orang yang tak berwenang tidak bisa masuk. Artinya kita mencegah lawan mendapatkan akses data anda dan mencegah orang dalam kampanye anda mengakses informasi yang tidak mereka butuhkan. Meskipun beberapa rekomendasi di bawah ini terlihat sulit dilakukan, para peretas mengintai mereka yang lebih mementingkan kenyamanan daripada keamanan.

APAKAH OTENTIKASI DUA FAKTOR ITU?

Otentikasi dua faktor merupakan lapisan keamanan kedua yang mewajibkan pengguna memberikan kredensial ekstra selain kata kuncinya. Faktor kedua ini sangat penting karena bila kata kunci anda dicuri, maka lawan masih bisa masuk ke dalam akun anda. Kata kunci merupakan sesuatu yang anda tahu dan faktor ke dua merupakan sesuatu yang anda miliki, misalnya kode yang dibuat oleh aplikasi, kunci fisik, atau sesuatu yang sifatnya biometrik, seperti sidik jari.

BAIK — Apa Yang Perlu Anda lakukan

1. Wajibkan otentikasi dua faktor (2FA) pada semua sistem dan aplikasi. Hindari pesan singkat untuk otentikasi dua faktor, karena penyerang dapat dengan mudah melakukan cloning terhadap nomor telefon dan mendapatkan akses ke pesan singkat. Ada beberapa aplikasi 2FA yang dapat digunakan sebaik pesan singkat, misalnya Google Authenticator, Microsoft Authenticator, dan Duo Mobile. Anda juga dapat menggunakan kunci fisik FIDO (“fast identity online”) yang dimasukkan ke dalam drive USB anda misalnya Yubikey atau Feitian. Laman “TwoFactorAuth.org” merupakan panduan yang berguna pada layanan-layanan yang mnawarkan maupun tidak 2FA.
2. Kata Kunci.
    a. Wajibkan kata kunci yang kuat. Seperti yang kita ingat di awal tadi “buatlah kata kunci yang panjang dan kuat”. Kemampuan komputer masa kini dapat memecahkan kata kunci tujuh karakter hanya dalam waktu millidetik. Kata kunci yang panjangnya 20 hingga 30 karakter akan membutuhkan waktu lebih lama bagi peretas untuk menerkanya. Pilih kata-kata yang dapat dengan mudah anda ingat.

b. Jangan ulang kata kunci! Gunakan kata kunci berbeda untuk akun yang berbeda, sehingga peretas tidak dapat masuk ke dalam berbagai akun anda bila satu kata kunci dicuri.

c. Agar staf dan sukarelawan kampanye terlindungi dari serangan phishing, hanya berikan kata kunci kepada orang yang bersangkutan atau melalui pesan terenkripsi dengan masa hidup yang singkat. Wajibkan pengaturan ulang kata kunci untuk akun utama melalui metode yang sama atau melalui chat video untuk memastikan bahwa benar yang meminta adalah staf atau sukarelawan. Jangan pernah bagi kata kunci melalui surat elektronik atau menyimpan/membagikannya melalui sistem helpdesk.

3. Gunakan manajer/pengelola kata kunci seperti LastPass, 1Password, atau Dashlane untuk membantu anda mengelola kata kunci yang panjang dan kuat dengan mudah. Namun pastikan sistem manajemen anda punya juga kata kunci yang panjang dan kuat, serta otentikasi dua faktor. Saat ini kami belum merekomendasikan manajer kata kunci yang digunakan melalui mesin peramban (browser) seperti Chrome, Safari dan Firefox, dimana seirngkali tidak seaman manajer yang secara eksklusif melakukannya.

4. Buatlah akun terpisah untuk administrator dan pengguna, dan batasi dengan ketat akses ke akun-akun administrator. Aministrator harus memiliki dua akun kampanye terpisah—satu yang digunakan oleh kegiatan admin mereka dans atu lagi yang menjadi akun standard untuk semua urusan kampanye. Ini akan mengurangi kemungkinan lawan mengganggu akun administrator, yang dapat mengakses jaringan secara keseluruhan.

5. Lakukan tinjauan periodik tentang siapa yang mengakses gawai dan jaringan manapun. Dengan segera ubahlah kata kunci bila terlihat ada kegiatan mencurigakan. Untuk memungkinkan hal ini terjadi, pastikan staf anda tidak berbagi akun pengguna.

MANAJER KATA KUNCI

Manajer kata kunci adalah salah satu cara menyimpan, mengambil dan menghasilkan kata kunci. Beberapa bahkan punya kemampuan untuk mengisi garis kata kunci pada halaman login. Manajer kata kunci membutuhkan kata kuncinya sendiri untuk masuk, yang menjadi kata kunci yang harus anda ingat. Risikonya tentu saja, bila ada yang masuk ke manajer kata kunci anda (dan ini pernah terjadi), orang itu akan memiliki semua kata kunci anda. Namun risiko ini selalu lebih kecil dari manfaatnya yaitu memiliki kata kunci yang kuat, unik untuk semua akun anda, dan dapat dikurangi secara signifikan dengan menggunakan otentikasi dua faktor pada manajer kata kunci anda. Untuk kampanye, manajer kata kunci dapat digunakan untuk akun yang punya banyak pengguna, karena administrator dapat dengan mudah mengaksesnya.

LEBIH BAIK — Ambil Langkah Berikutnya

1. Buat profil pengguna untuk setiap jenis staf kampanye yang secara otomatis mendapatkan tingkatan akses yang dibutuhkan. Berbagai jenis pegawai—sukarelawan, pemagang, staf lapangan, pemimpin kampanye—membutuhkan akses untuk berbagai sumber yang berbeda. Dengan adanya profil yang sudah ditentukan sebelumnya, maka lebih mudah memastikan mereka mendapatkan akses pada hal-hal yang benar mereka butuhkan.

APAKAH ADMINISTRATOR ITU?

Dalam “Bahasa IT”, “administrator” atau “admin” memiliki kemampuan untuk memberikan akses atau kendali kepada siapapun ke sistem atau informasi. Contohnya, sebagai “admin” untuk sistem surel, anda dapat membuat akun, mengganti kata kunci, dan mengatur persyaratan seperti panjangnya kata kunci, dan otentikasi dua faktor untuk semua akun. Pada office suit seperti Gsuite atau Microsoft365 anda dapat membuat grup, misalnya “Tim Lapangan” atau “Tim Komunikasi”. Tugas admin sangat penting. Bila mereka melakukan kerja mereka dengan benar, maka informasi yang tepat akan tersedia untuk mereka yang membutuhkan, yang sangat penting untuk keamanan. Artinya memutuskan siapa yang mendapatkan keistimewaan admin juga menjadi keputusan penting. Hanya sedikit orang yang terpercaya dan terlatih yang harus memiliki kemampuan memberikan ijin kepada orang lain untuk mengakses informasi. Bila keistimewaan staff atau admin keluar dari kampanye, pastikan anda juga ambil kembali keistimewaan itu dari mereka!

Langkah 4: Perencanaan Tanggap Insiden

Membuat rencana tanggap setelah serangan sama pentingnya dengan mengembangkan strategi keamanan untuk mencegah serangan. Bagaimana anda menanggapinya erat kaitannya dengan apa dampak yang ditimbulkan oleh insiden tersebut ketimbang dari kerusakan apa yang terjadi. Anda harus meluangkan waktu dengan para pemimpin atau manajemen senior untuk membahas apa yang terjadi bila ada yang salah. Berikut ini adalah daftar periksa berisi langkah-langkah yang harus anda lakukan:

HUKUM

tentukan di luar dewan, siapa yang akan anda pertahankan saat terjadi insiden di dunia maya, dan bahaslah proses tanggap kejadian dengan mereka sejak awal kampanye. Pada banyak kasus, ini adalah orang yang sama yang mewakili kampanye anda pada hal lainnya, namun idealnya anda harus punya orang khusus yang bersiap menanggapi insiden setiap saat, baik yang bekerja secara pro bono atau dibayar sebesar $0.

minta pengacara anda menjelaskan kewajiban hukum bila data dicuri dan tindakan-tindakan kepatuhan apa yang harus anda miliki.

Pahami kewajiban hukum vendor anda untuk memberitahu anda atau yang lain bila mereka diretas. Sedapat mungkin, masukkan persyaratan pemberitahuan yang ketat, karena pihak ketiga merupakan sumber pelanggaran yang paling sering terjadi.

Bila anda yakin anda sudah dilanggar, praktik terbaik adalah pengacara anda mengawasi tanggapan anda seeperti yang diatur dalam hubungan istimewa antara pengacara-klien

bicarakan dengan pengacara anda tentang cara terbaik untuk bekerja dengan penegak hukum bila terjadi pelanggaran. Setiap kampanye akan memiliki pendekatannya sendiri.

TEKNIS

Tentukan sejak awal siapa yang akan anda hubungi untuk mendapatkan bantuan teknis bila anda diretas.

Pilih siapa dari kampanye anda yang akan berhubungan dengan ahli teknis bila terjadi pelanggaran. Idealnya, ini adalah orang yang sama yang sudah berkoordinasi masalah IT untuk kampanye. Mengelola tanggap insiden bisa menyulitkan, jadi anda mau seseorang yang dapat fokus pada aspek teknis yang tahu persis apa yang mereka lakukan. Dengan demikian, anda bisa fokus pada komunikasi dengan para pemangku kepentingan dan media massa.

ketahui tentang bantuan teknis atau bantuan lain yang dapat disediakan oleh penyedia platform ketika terjadi insiden di dunia maya misalnya peretasan atau serangan lain.

OPERASIONAL

Putuskan sejak awal siapa yang akan menjadi bagian dari Tim Tanggap Insiden anda, dan siapa yang akan berpartisipasi dalam pertemuan tanggap insiden. Penting untuk mengikutsertakan personil dari tim IT, Legal, operasional dan komunikasi. Bila kampanye anda kecil, dan tidak punya tim komunikasi, IT atau operasional yang purna waktu, rencanakan untuk mengikutsertakan staf penting yang akan mengawasi operasional kampanye.

Tentukan rantai komando untuk pengambilan keputusan saat terjadi pelanggaran, terutama yang berkaitan dengan komunikasi. Di banyak kasus, ini adalah manajer kampanye, namun beberapa manajer dapat memilih untuk mendelegasikan tanggungjawabnya kepada orang lain.

tentukan aplikasi atau teknologi apa yang akan anda gunakan untuk berkomunikasi bila sistem anda dilanggar. Misalnya, bila surel anda diretas, anda akan bergantung pada platform pengiriman pesan yang aman, misalnya Signal atau Wickr. Penting untuk terus berkomunikasi saat terjadi pelanggaran, namun tentu anda tidak ingin lawan anda tahu apa yang anda bicarakan,--atau bahkan mengetahui anda sedang menanggapi aksi mereka.

KOMUNIKASI

Lakukan perencanaan skenario. Bagi banyak kampanye, ini bisa menjadi bagian dari pemunduran strategi. Untuk kampanye yang lebih besar dengan risiko yang lebih tinggi, mungkin perlu ada pertemuan khusus.

Identifikasilah para pemangku kepentingan internal dan eksternal yang utama, seperti staf, sukarelawan, donor dan pendukung anda. Ketahui siapa yang harus anda hubungi bila terjadi insiden dan beri peringkat sesuai dengan urutan prioritas. Kembangkan daftar nara hubung dan tunjuk siapa yang akan menghubungi mereka.

Lakukan curah pendapat tentang skenario yang paling merusak dan pertimbangkan bagaimana pemangku kepentingan anda dan penyampaian pesan berubah untuk masing-masing pemangku kepentingan itu. Skenario yang berbeda dapat termasuk:

- Selentingan bahwa kampanye anda diretas;
- Informasi pribadi pendukung anda bocor;
- Informasi keuangan yang sensitif dari donor anda dicuri, misalnya nomor kartu kredit dan informasi narahubungnya;

- Permintaan ransum dan pemerasan terhadap kampanye anda;
- Sistem anda dihapus dan dimatikan;
- Surel seseorang dicuri;
- Lawan anda mencuri informasi penting milik administrator anda dan setiap file yang ada di dalam drive kampanye anda;
- Akun media sosial anda diturunkan atau diretas;
- Internetnya terputus, atau laman, aplikasi atau protokol tertentu diblok di seluruh negeri;
- Akses terhadap informasi penting diblok atau diganggu oleh penyensoran..

Berhati-hatilah dengan apa yang anda ucapkan tentang kebijakan keamanan dunia maya atau insiden dunia maya. Beberapa korban kejahatan dunia maya sudah membuat pengumuman besar-besaran mengenai tindakan keamanan mereka, atau mengkritisi mereka yang diserang. Media massa akan meminta pertanggungjawaban akan apa yang anda katakan di masa lalu bila anda bermain sebagai korban.

Demikian pula, hindari memberian cakupan kejadian secara rinci pada masa-masa awal insiden (dan bila anda dapat menghindari membahas seberapa besar kejadiannya bahkan lebih baik lagi). Detil yang muncul saat awal insiden akan mengalami banyak perubahan seiring dengan penyelidikan yang anda lakukan. Kesalahan yang paling sering terjadi adalah mengatakan sesuatu yang ternyata tidak benar (misalnya: "tidak banyak yang mereka curi," atau "tidak ada informasi pribadi yang diambil). Katakan hanya yang anda ketahui pasti merupakan jalan teraman. Pernyataan harus fokus pada tindakan yang anda ambil untuk memperbaiki situasi bagi para pemangku kepentingan yang terdampak.

Kembangkan pernyataan-pertanyaan yang mungkin muncul sebelumnya, idealnya berkonsultasi dengan perwakilan hukum anda, sehingga anda dapat membuat peryataan atau butir bicara dengan cepat bila kejadian terjadi. Setidaknya buatlah dokumen T&J sederhana yang dapat dengan mudah anda revisi bila anda membutuhkannya. Membuat dokumen T&J sebelumnya akan membantu anda berpikir panjang tentang hal-hal yang tidak anda katakan daripada yang anda katakan. Misalnya, biasanya pertanyaan pertama adalah, "Apa yang terjadi?" Namun anda mungkin tidak bisa menjawabnya dalam beberapa hari atau bahkan minggu ke depan. Fakta bahwa anda tidak tahu pelanggaran seperti apa yang trjadi akan membantu anda menuliskan jawaban-jawaban yang mungkin muncul sebelumnya.

PERTANYAAN-PERTANYAAN YANG ADA DALAM DOKUMEN T&J ANDA MISALNYA:

- Apa yang terjadi?
- Bagaimana terjadinya?
- Siapa yang melakukannya?
- Apa yang dicuri atau rusak?
- Apakah ada informasi pribadi yang dicuri? Apa yang anda lakukan untuk melindunginya?
- Bagaimanakah para peretas melakukannya?
- Apakah peretas itu di luar sistem anda?
- Berapa lama mereka berada di sistem anda?
- Tindakan-tindakan pengamanan seperti apa yang anda punya? Mengapa itu semua tidak efektif?
- Bukankah seharusnya anda tahu ini akan terjadi? Mengapa sistem anda tidak diamankan lebih baik lagi?
- Apakah anda bekerjasama dengan penegak hukum? Apakah mereka sudah menghubungi anda?
- Bila pelanggaran ini disertai permintaan tebusan, anda akan ditanyai: apakah anda membayar tebusannya, dan mengapa iya atau tidak?

Tetap jaga hubungan baik dengan para pemangku kepentingan utama dan sedapat mungkin selalu berikan informasi bagi mereka. Mungkin anda tidak akan banyak mengatakan apapun, namun secara teratur hubungi mereka dengan informasi yang anda ketahui, anda punya pernyataan jelas tentang niat anda, dan berikan rincian tentang apa yang anda lakukan untuk mengatasi hal tersebut menjadi hal yang penting. Hindari membuat ekspektasi dari berita terkini yang terlalu sering karena terkadang anda tidak punya informasi baru dan para pemangku kepentingan anda akan semakin frustrasi bila anda datang tanpa informasi baru. Bicara secara proaktif kepada media hanya bila anda punya informasi baru.

Langkah 5: Gawai

Setiap gawai fisik dalam kampanye anda—mulai dari telefon genggam, tablet, atau laptop hingga router, printer atau kamera—merupakan jalur penyerangan potensial ke jaringan anda. Rencana keamanan dunia maya yang baik akan berupaya mengendalikan akses ke dan di seluruh gawai. Anda dapat mengendalikan akses pada gawai dengan memastikan gawai tersebut ditangani dengan baik dan selalu ada yang dapat mempertanggungjawabkan keberadaannya. Anda dapat mengendalikan akses melalui otentikasi dua faktor dan kata kunci yang kuat. Anda mengendalikan konten gawai melalui enkripsi dan kebijakan yang memandu bagaimana anda menyimpan data (dalam hal ini menyimpan informasi di cloud dan bukan mesin).

BAIK — Apa Yang Perlu Anda lakukan

1. Selalu gunakan sistem operasional yang paling terbaru, karena pembaruan sistem secara teratur juga memperbaiki kerentanan-kerentanan terkini. Bila mungkin, atur gawai untuk memasang pembaruan ini secara otomatis. Jadikan salah satu uraian pekerjaan staf adalah memastikan secara teratur OS yang digunakan adalah yang terkini.

2. Siapkan Backup! Untuk data apapun yang anda simpan di gawai lokal (PC misalnya), pastikan ada rencana cadangan bila ada pencurian fisik, bila komputer anda rusak, atau secara tak sengaja anda menumpahkan kopi ke papan kunci anda. Misalnya, anda dapat menggunakan layanan backup berbasis cloud yang otomatis untuk memitigasi dampak dari kehilangan data. Misalnya Backblaze dan CrashPlan.

3. Akses terhadap gawai

    a. Sejak awal, pimpinan kampanye harus dapat menciptakan lingkungan dimana semua orang menganggap keamanan fisik secara serius—gawai yang hilang dapat membuka akses lawan terhadap informasi penting yang dapat mereka gunakan untuk menciderai kampanye anda.

    b. Meskipun banyak kampanye yang tidak mampu membeli gawai baru, membeli peralatan baru selalu menjadi pilihan terbaik (terutama komputer dan telefon) bila anda mampu. Setidaknya, anda memberikan gawai baru untuk personil yang menangani data sensitif atau setidaknya menghapus dan menginstal ulang sistem operasional baru untuk gawai-gawai lama. Bila staf menggunakan komputer dan telefon mereka sendiri, buatlah kebijakan “Bring Your Own Device” (BYOD) yang melaksanakan praktik keamanan kuat (lihat perlindungan pada endpoint di bawah ini).

    c. Para anggota kampanye TIDAK boleh menggunakan akun atau gawai pribadi yang belum diamankan seperti yang diatur dalam kebijakan BYOD untuk urusan kampanye, termasuk

surel dan medsos. Informasi penting apapun yang berada di luar gawai atau sistem yang dikendalikan oleh kampanye rentan mengalami serangan. Pimpinan harus secara terus menerus menegaskan bahwa data kampanye tidak boleh disimpan di surel pribadi dan komputer yang tidak aman.

d. Selalu perhatikan keamanan fisik gawai-gawai anda. Ketika berada di transportasi publik, di kafe, atau bahkan di kantor anda sendiri, selalu ambil langkah-langkah untuk mencegah pencurian gawai yang akan dapat mengakses akun, komunikasi dan data anda.

e. Laporkan kehilangan gawai sesegera mungkin. Wajibkan pengaturan yang memungkinkan penghapusan jarak jauh semua gawai. Misalnya masukkan Find my iPhone dan Android Device Manager.

f. Menang atau kalah, buatlah rencana untuk menentukan apa yang terjadi terhadap semua data, akun dan gawai ketika kampanye berakhir. Masa setelah kampanye berakhir merupakan masa yang paling rentan.

4. Mengakses gawai

a. Ubah kata kunci dan pengaturan di seluruh gawai. Banyak gawai sudah punya kata kunci dari pabrik yang mudah diterka. Juga, buatlah akun tamu tidak dapat digunakan bila gawai memungkinkannya.

b. Terapkan ‘auto-lock’ untuk telefon dan komputer setelah dua menit dan wajibkan memasukkan kata kunci atau sidik jari untuk membukanya.

c. Nyalakan fitur ‘auto-wipe’ untuk gawai anda sehingga data akan terhapus dengan sendirinya setelah beberapa kali upaya login gagal.

5. Konten pada gawai

a. Wajibkan enkripsi untuk semua gawai (komputer dan telefon) untuk memastikan hilangnya gawai tidak berarti konten atau isinya berisiko. Contohnya FileVault untuk Mac dan BitLocker untuk Windows. Beberapa gawai seperti iPhone melakukannya by default, tapi tidak semua begitu.

b. Pasang piranti lunak perlindungan endpoint untuk semua gawai. Beberapa contoh diantaranya Trend Micro, Sophos dan Windows Defender. Ada beberapa aplikasi keamanan endpoint untuk telefon dan komputer tablet, misalnya Lookout.

APAKAH PERLINDUNGAN ENDPOINT ITU?

Endpoint adalah gawai yang digunakan oleh staf, termasuk telefon selular, komputer laptop dan komputer desktop. Kesemua gawai tersebut adalah ‘endpoint’ dari jaringan kampanye, dan staff adalah “end user”. Perlindungan endpoint secara terpusat mengontrol dan mengelola keamanan dari gawai-gawai jarak jauh. Hal ini penting untuk kampanye yang memperkenankan staf mereka ‘membawa gawai sendiri’ (BYOD), karena kampanye harus memastikan gawai itu aman, bebas dari malware, dan dapat dihapus bila dicuri atau hilang. Perlindungan endpoint juga memantau gawai untuk memastikan piranti lunaknya terkini dan mendeteksi malware baru atau ancaman potensial lainnya. Bagi banyak kampanye, hal ini akan terasa berat awalnya, namun membangun kebiasaan ini saat merekrut staf dan melakukan investasi di awal akan membuat anda terhindar dari rasa penyesalan mendalam.

LEBIH BAIK — Lakukan Langkah Selanjutnya

1. Gunakan piranti lunak untuk mengelola gawai selular (MDM), yang memantau kegiatan yang memastikan semua gawai patuh pada kebijakan keamanan gawai dan telefon selular yang anda buat untuk kampanye anda. Contohnya VMware AirWatch, Microsoft InTune, dan JAMF. GSuite dan Microsoft Office 365 juga punya layanan MDM.

2. Gunakan layanan perlindungan terhadap ancaman yang memantau dan memberikan peringatan bila ada aktivitas yang mencurigakan, misalnya CrowdStrike Falcon or Mandiant FireEye. Crowdstrike terkadang menawarkan layanan perlindungan pelanggaran Falcon secara pro bono melalui Crowdstrike Foundation, bergantung pada kebutuhan kampanye anda dan aturan pembiayaan kampanye.

Langkah 6: Jaringan

Jaringan adalah sistem piranti keras fisik, piranti lunak digital dan koneksinya. Jaringan merupakan lingkungan yang seringkali menjadi sasaran empuk serangan. Keamanan jaringan terdiri dari semua mulai bagaimana gawai berkomunikasi satu sama lain hingga penggunaan layanan berbasis cloud untuk penyimpanan data.

BAIK — Apa Yang Perlu Anda lakukan

1. Simpan data pada layanan berbasis cloud yang terpercaya, bukan pada komputer atau server personal. Apapun yang anda simpan di gawai pribadi, akan lebih berisiko mengalami peretasan, pencurian, kecelakaan atau perampasan dibandingkan dengan data yang disimpan di cloud.
    a. Tidak semua orang bisa mengakses semua file dalam jaringan; akun dengan akses administrator menyeluruh tidak boleh digunakan untuk kegiatan sehari-hari. Bagi penyimpanan file anda berdasarkan folder departemen dan berikan akses seperlunya.
    b. Pastikan akses konten bersama hanya dapat berdasarkan undangan saja. Beberapa layanan pengelolaan file memberikan peluang untuk memberlakukan tanggal kadaluwarsa pada undangan dan akses.
    c. Secara periodik audit apa saja yang dibagi bersama dan dengan siapa.
2. Buat jaringan wifi "tamu" terpisah bagi para pengunjung dan sukarelawan yang akan membatasi akses mereka terhadap sumberdaya kampanye. Cobalah beli router yang menawarkan "profil tamu" yang secara otomatis membuat segment jaringan anda. Kami sangat menyarankan mengubah kata kunci jaraingan di akhir kampanya ketika jumlah staf berubah secara besar-besaran.
3. Ketika anda melakukan perjalanan, atau sebelum anda membangun kantor kampanye, hindari layanan wifi publik sedapat mungkin dan gunakan hanya jaringan wifi terpercaya. Bila anda membutuhkan koneksi wifi yang mobile, cobalah sediakan hotspots wifi mobil untuk tethering bagi para staf kampanye. Wifi publik biasanya gratis dan mudah untuk koneksi, namun para penyerang juga dapat menggunakannya untuk masuk ke dalam piranti keras anda.
    a. Sedapat mungkin para staf harus menggunakan VPN (jaringan maya pribadi). VPN membantu melindungi dari orang asing ketika menggunakan wifi publik. Contoh dari layanan VPN ini termasuk ExpressVPN atau TunnelBear. Tidak semua VPN sama. Berhati-hatilah pada layanan yang gratis: banyak yang sengaja ingin mengambil data anda!
4. Amankan browser (mesin peramban) anda. PC Magazine memberikan peringkat sebagai mesin peramban teraman bagi Chrome dan Firefox pada tahun 2017. Apapun peramban yang anda gunakan, selalu perbarui.

APAKAH VPN ITU?

Virtual Private Network (VPN) adalah “terowongan” terenkripsi bagi lalu lintas internet anda, menyembunyikannya dari kemungkinan orang memasuki jaringan anda. Beberapa kantor menggunakannya sebagai cara untuk masuk secara jarak jauh ke jaringan kantor, namun ini belum terlalu umum bagi kampanye. Kampanye harus mempertimbangkan penggunaan VPN bagi para staf mereka di komputer atau telefon selular bila mereka sering menggunakan wifi publik atau jaringan yang tidak bisa dipercaya (yang terkadang sering dialami oleh staf yang bepergian atau berada di kantor lapangan). Google baru-baru ini mengeluarkan sistem VPN yang bisa dilakukan sendiri bernama Outline.

LEBIH BAIK — Ambil Langkah Berikutnya

1. Anda dapat mengambil langkah-langkah yang lebih jauh untuk melindungi jaringan anda, namun semua langkah ini sebaiknya dijalankan oleh professional di bidang IT. Kami sarankan anda meminta mereka untuk memasukkan beberapa hal berikut:
    a. Buat hardware firewall.
    b. Enkripsi koneksi wifi anda dengan menggunakan WPA2 atau protokol keamanan (jangan gunakan WEP).
    c. Buatlah konfigurasi proxi web berbasis cloud untuk memblok akses ke laman-laman mencurigakan dari gawai yang dimiliki oleh kampanye, dimanapun lokasinya. Beberapa contoh penyedia layanan adalah Zscaler, Cisco Umbrella dan McAfee Web Gateway Cloud Service.
    d. Simpanlah log kegiatan anda di penyedia layanan cloud seperti LogEntries atau SumoLogic.
    e. Buat segment dalam penyimpanan berbasis cloud sehingga anda tidak menyimpan semua di tempat yang sama. Penelitian oposisi, memo strategi, dan berkas-berkas personil harus disimpan di folder yang berbeda, dan akses terhadap folder tersebut hanya terbatas pada mereka yang benar-benar membutuhkannya. Pertimbangkan untuk menggunakan sistem penyimpanan yang sama sekali berbeda untuk informasi yang paling sensitif dari kampanye anda. Batasi akses sehingga hanya orang-orang tertentu yang dapat mengaksesnya, dan hanya menggunakan alat khusus. (Misalnya bila anda menggunakan Microsoft365 untuk office suite dan penyimpanan dokumen anda, letakkan dokumen yang paling sensitif di Dropbox atau akun box). Bila anggota kampanye menghadapi risiko, segmentasi seperti ini akan mengurangi kerusakannya.
2. Latih staf anda untuk tidak menghubungkan gawai mereka dengan port atau gawai yang tidak dikenal. Jangan gunakan alat pengisi batere publik di bandara atau acara-acara. Jangan terima alat pengisi batere atau batere di acara (drive USB cuma-cuma itu mungkin berisi malware!).

Langkah 7: Operasi Informasi dan Komunikasi Menghadapi Publik

Operasi informasi sudah cukup lama beredar di berita, terutama untuk kampanye-kampanye yang dijalankan oleh layanan intelejen asing. Menjadi pilihan para pemimpin terpilih dan pembuat kebijakan bagaimana menghadapi operasional informasi di masa yang akan datang dan tak banyak yang bisa kita lakukan sebagai staf kampanye apakah benar terjadi atau tidak, namun ada yang bisa kita lakukan untuk menanganinya bila terjadi. Kampanye akan terus menjadi sasaran dari operasi-operasi semacam ini dan harus bersiap siaga. Membela bagaimana kampanye anda berkomunikasi dengan publik menjadi bagian penting. Di bawah ini ada beberapa cara untuk melindungi kampanye anda dari operasional informasi, identifikasi ketika terjadi pada kampanye atau kandidat anda dan tanggapi dengan cepat ketika benar terjadi.

APAKAH OPERASI INFORMASI ITU?

Informasi merupakan kekuatan—atau setidaknya itu yang dipercayai oleh banyak militer dan intelejen! Kekuatan gagasan telah lama menjadi bahan bakar pemberontakan, makar dan perang saudara dan banyak negara yang mungkin memiliki kemampuan militer yang rendah secara tradisionl akan berusaha untuk menggunakan informasi untuk memecah belah dan menaklukkan lawan-lawan mereka. Di Russia, contohnya, memengaruhi pendapat publik melalui propaganda dan menyulut ketegangan lokal merupakan bagian dari doktrin perang mereka dan sesuatu yang seringkali mereka gunakan untuk lawan-lawan mereka. Media sosial mengubah wajah permainan operasi informasi ini. Kini jauh lebih mudah untuk memindahkan informasi dengan cepat dan menyerupai orang lain, menciptakan kesan kemarahan atau perpecahan masyarakat.

BAIK — Apa Yang Perlu Anda lakukan

1. Ingat: Operasi Informasi merupakan permasalahan komunikasi, bukan masalah teknis. Para lawan dapat membuat operasi informasi mereka makin ampuh dengan mencuri data anda, namun begitu informasi ini keluar, anda butuh strategi komunikasi untuk mengelolanya. Pikirkan terlebih dahulu bagaimana caranya menangani kabar burung atau fitnah—apakah anda akan mengabaikannya? Meretweet dan menegaskan bahwa itu salah? Bagaimana anda membuat keputusan ini? Ini adalah keputusan-keputusan tersulit yang harus

diambil oleh tim kampanye, namun yang paling penting adalah pertanyaan-pertanyaan dalam tim anda sebelumnya, sehingga anda dan tim anda memiliki panduan bagaimana menanggapinya, bila anda menanggapi semua itu.

2. Ketahui apa yang sedang terjadi. Dorong para aktifis untuk berbagi post, laman, atau cerita berita yang menurut mereka mencurigakan. Bila anda mau, anda dapat menugaskan beberapa pemagang atau sukarelawan untuk fokus pada hal ini secara khusus, melakukan pencarian untuk mencari tahu konten apa yang ada di luar sana. Salah satu tantangan terbesar adalah tidak mungkin kita mengetahui apa saja yang dibaca oleh pemilih di laman Facebook mereka. Platform ini memang membuat semakin sulit untuk mengunggah iklan politik dan meningkatkan jumlah staf yang memantau konten berita, namun anda tidak bisa mencari semua konten. Cara terbaik untuk menyelesaikan hal ini adalah untuk menugaskan tim sukarelawan yang mewakili berbagai daerah dan kelompok demografi di daerah anda sehingga anda bisa menangkap semua berita sebanyak mungkin.

3. Bangun hubungan dengan platform medsos utama dan beritahu mereka bila anda menemukan informasi palsu atau menyesatkan. Sebagian besar platform medsos kini akan menghilangkan konten yang "palsu" atau menyesatkan dan profil-profil yang menipu. Tanyakan kepada komite kampanye atau pihak negara narahubung yang terbaik dari platform medsos dan bangun hubungan sejak awal kampanye sehingga anda dapat menjangkau dengan cepat bila ada sesuatu yang tidak benar.

    a. Facebook

    b. Twitter

    c. Google/Youtube

4. Pantau Laman-laman penipu. Hingga saat ini, belum ada laporan mengenai penipu yang mencuri uang atau data aktifis melalui laman palsu, namun laman bisa menjadi vektor serangan yang paling efektif, anda harus berhati-hati. Pastikan untuk membeli alamat laman yang akan anda gunakan (atau dapat digunakan untuk melawan anda). Bila anda mau, anda bisa mendapatkan layanan manajemen reputasi yang akan memantau laman untuk anda. Beberapa dapat melakukannya dengan harga yang murah.

5. Lindungi diri anda dari Distributed Denial of Service Attack (dikenal sebagai DDos). Serangan DDoS adalah ketika lawan anda mengendalikan banyak mesin, dan menggunakannya untuk 'ping' laman anda pada saat bersamaan, membuatnya rusak. Dalam panduan ini kami lebih banyak berfokus pada bagaimana menjaga agar orang tidak menyentuh data kampanye anda, namun bila terjadi Ddos, anda harus membiarkan laman anda terbuka, dan tersedia setiap saat untuk donor dan aktifis. DdoS belum menjadi ancaman kampanye yang umum, namun dapat digunakan untuk memblok anda dari mendapatkan penggalangan dana atau menyebabkan gangguan terhadap kampanye anda. Ada banyak alat gratis yang dapat anda gunakan untuk melindungi laman anda seperti Google Shield dan Cloudflare.

Apakah Anda punya ide untuk membuat Playbook ini lebih baik?

Apakah ada teknologi baru atau hal-hal sensitif lain yang harus kami tangani?

Kami ingin anda memberikan umpan balik anda.

Mohon dapat berbagi gagasan, cerita dan komentar anda di Twitter @d3p dengan memberikan tagar #CyberPlaybook atau kirimkan surat elektronik ke connect@d3p.org sehingga kami dapat memperbaiki sumber informasi ini seiring dengan perubahan lingkungan digital di dunia ini.

Melindungi Demokrasi Digital
Pusat Belfer untuk Sains dan Hubungan Internasional
Sekolah Pemerintahan John F. Kennedy

79 JFK Street
Cambridge, MA 02138
www.belfercenter.org/D3P

www.belfercenter.org/D3P