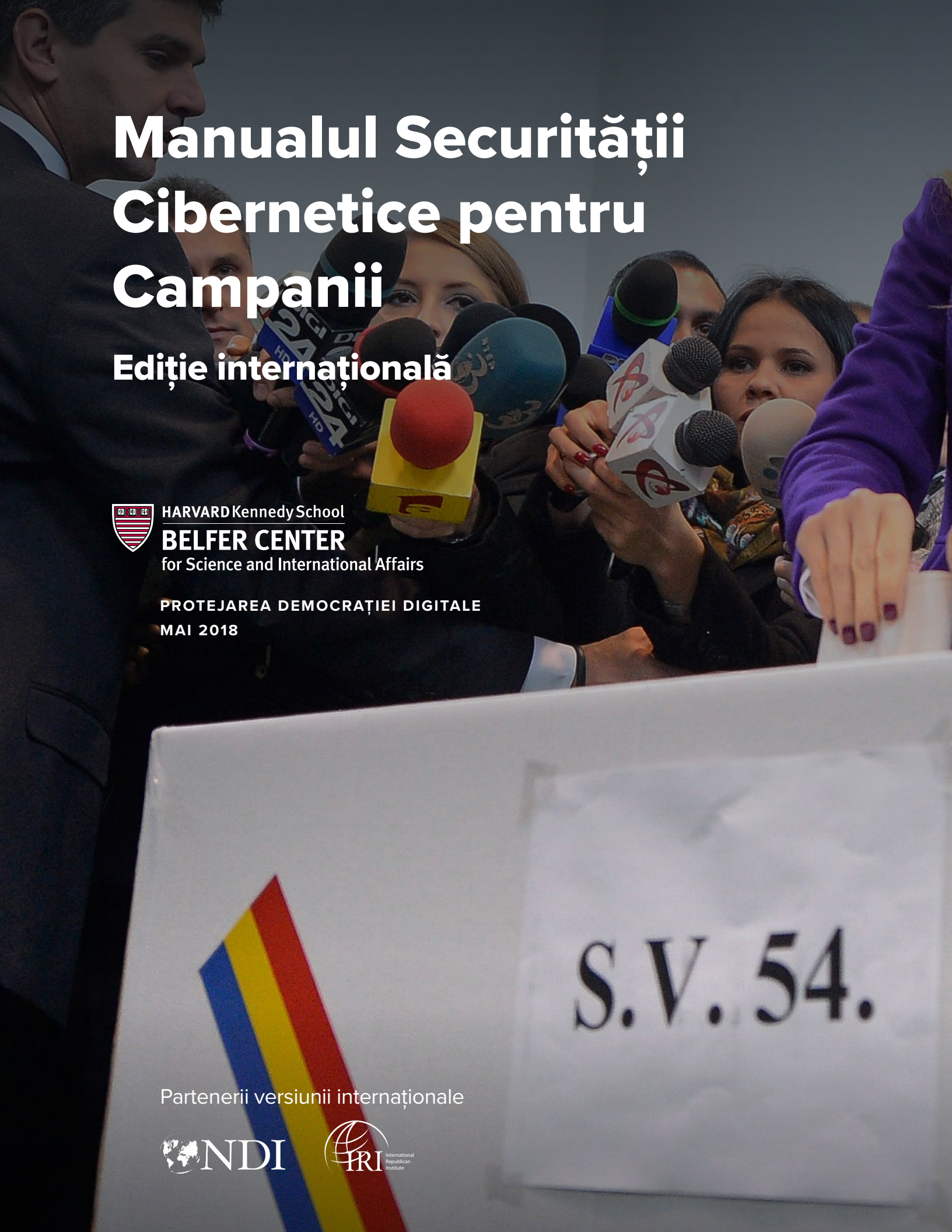

Manualul Securității Cibernetice pentru Campanii

Ediție internațională

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PROTEJAREA DEMOCRAȚIEI DIGITALE

MAI 2018

Partenerii versiunii internaționale

NDI

IRI International Republican Institute

Defending Digital Democracy Project
Protejarea Democrației Digitale
Centrul Belfer de Știință și Relații Internaționale
Școala de guvernare John F. Kennedy

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

Partenerii versiunii internaționale:

Institutul Național Democratic
www.ndi.org

Institutul Internațional Republican
www.iri.org

Declarațiile și atitudinile exprimate în acest document reflectă doar opinia autorului și nu reprezintă poziția Universității Harvard, a Școlii de Management John F. Kennedy sau a Centrului pentru Știință și Relații Internaționale Belfer.

Design și aspect—Andrew Facini

Fotografie pe copertă: Conferință de presă la deschiderea unei secții de votare în România. (AP / Octav Ganea)

Last updated 2018-12-04

Copyright 2018, President and Fellows of Harvard College

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PROTEJAREA DEMOCRAȚIEI DIGITALE
MAI 2018

Manualul Securității Cibernetice pentru Campanii

Ediție internațională

Cuprins

Cuvânt de salut

Oamenii se alătură campaniilor din diferite motive: alegerea unui lider în care ei cred, promovarea unei agende, curățirea guvernului sau pentru a simți adrenalina și agitația din viața unei campanii. Acestea sunt câteva dintre motivele pentru care ne-am implicat în viața politică. Cu siguranță nu ne-am implicat pentru că am vrut să devenim experți în cibernetică și presupunem că nici Dvs. nu ați făcut-o.

Din păcate, numărul amenințărilor la adresa securității este în creștere și ele au puterea de a vă deturna complet campania. Venim din lumea campaniilor și susținerii proceselor democratice internaționale și am văzut din propria experiență felul în care hacking-ul, dezinformarea și spargerea website-urilor pot afecta cursul alegerilor—și direcția unei țări.

D3P este o echipă de experți bipartizani în domeniul securității cibernetice în domeniile publice și private, precum și experți în campani electorale. Pentru această ediție, am colaborat cu Institutul Internațional Republican (IRI) și Institutul Național Democrat (NDI) pentru a înțelege mai bine peisajul electoral internațional și cum să ne protejăm împotriva riscurilor digitale

Venim din diferite partide politice și avem păreri diferite când vine vorba despre politici publice, dar lucrul care ne unește este convingerea că alegătorii trebuie să decidă cursul alegerilor și nu altcineva. Modul nostru de viață și de lucru tot mai digital, oferă adversarilor noștri noi modalități de a influența campaniile și alegerile. Nu trebuie să fiți un expert cibernetic pentru a organiza o campanie de succes, însă aveți responsabilitatea de a vă proteja candidatul și organizația de adversarii din spațiul digital. De aceea, Apărarea Democrației Digitale, un proiect al Centrului de Științe și Afaceri Internaționale din Belfer al Școlii Harvard Kennedy, a creat acest manual de prezentare a campaniei.

Institutul Național Democratic, Institutul Internațional Republican și zeci de oficiali aleși, experți în securitate și profesioniști de campanie au lucrat la Proiectul Apărarea Democrației Digitale și au adaptat acest manual pentru un context internațional mai larg

Informațiile adunate aici sunt pentru orice campanie, a oricărui partid. Acesta a fost conceput pentru a vă oferi cunoștințe simple și aplicabile care vă vor ajuta să protejați campania Dvs. de

cei care încearcă să vă atace organizația—și democrația țării Dvs. Mai presus de toate, sperăm că acest manual vă va permite să dedicați mai mult timp principalului Dvs. obiectiv—campania.

Mult succes!

Robby Mook
Managerul campaniei Hillary Clinton 2016.

Matt Rhoades
Managerul campaniei Mitt Romney 2012.

P.S. — Aveți idei pentru îmbunătățirea acestui manual? Există tehnologii sau vulnerabilități noi pe care ar trebui să le abordăm? Așteptăm părerea Dvs. Vă rugăm să ne împărtășiți ideile, istoriile și comentariile Dvs. pe Twitter @d3p folosind hashtag-ul #CyberPlaybook sau să ne trimiteți un e-mail la adresa connect@d3p.org, pentru a continua îmbunătățirea acestui manual pe măsură ce mediul digital se schimbă.

Autori și Contribuitori

Acest proiect a fost posibil datorită autorilor care au donat generos timpul lor.

Mulțumiri speciale pentru **Debora Plunkett**, care a coordonat acest proiect și pentru **Harrison Monsky** pentru scrierea documentului. Le suntem recunoscători și oamenilor menționați mai jos, care au investit nenumărate ore pentru a redacta și îmbunătăți acest manual.

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

Abordarea Manualului

Acest manual al Securității Cibernetice în Cadrul Campaniei Electorale a fost scris de o echipă de experți internaționali, din diferite partide, în securitate cibernetică, politică și drept, pentru a oferi modalități simple și aplicabile de combatere a amenințărilor cibernetice, care sunt în creștere.

Adversarii cibernetici nu discriminează. Au fost sparte campanii de toate nivelurile, nu doar naționale. Ar trebui să presupuneți că sunteți o țintă. Cu toate că recomandările din acest manual sunt universale, ele sunt în primul rând indicate pentru campaniile care nu dispun de resurse pentru a angaja personal profesionist în domeniul securității informaționale. Oferim elemente de bază ale strategiei de reducere a riscului la adresa securității informaționale, pe care oamenii fără instruire tehnică le pot implementa (deși am inclus și unele elemente care vor necesita ajutorul unui profesionist în domeniul IT).

Acestea sunt niște recomandări de bază și nu reprezintă un set complet de referințe pentru a obține cel mai înalt nivel de securitate posibil. Încurajăm toate campaniile să recurgă la ajutorul profesional al specialiștilor din domeniul IT și securității cibernetice ori de câte ori este posibil.

Introducere

Candidații și campaniile se confruntă cu o serie amplă de provocări. Sunt multe evenimente de organizat, voluntari de recrutat, ședințe publice de gestionat, fonduri de colectat, alegători de contactat și nenumărate cerințe ale ciclului media modern. Fiecare membru al echipei trebuie să anticipeze surprizele neașteptate, cum ar fi gafele sau un atac pe ultima sută de metri. În zilele noastre, această listă include și atacurile cibernetice, campaniile de dezinformare și cenzura internetului.

Pe măsură ce campaniile devin din ce în ce mai digitale, adversarii găsesc noi oportunități de a interveni, a deturna și a fura. În 2008, hackerii chinezi s-au infiltrat în campaniile lui Obama și McCain și au furat de la ambele cantități enorme de informații. În 2016, rețelele sociale din Uganda au fost deconectate în timpul alegerilor. În 2016, operatorii cibernetici, care se presupune că ar fi fost sponsorizați de guvernul Rusiei, au furat și au scurs zeci de mii de e-mailuri și

documente de la personalul de campanie al Partidului Democrat din SUA, alimentând campanii de dezinformare distructive. În 2017, partidele politice din Kenya s-au confruntat cu o serie lungă de campanii de dezinformare, iar pagina Facebook a unui partid politic important din Serbia a fost deconectată.

Consecințele unui atac cibernetic pot fi substanțiale. Știrile despre atac în sine, însoțite de o publicare lentă, de-a lungul unei perioade îndelungate, a informației furate, pot afecta mesajul unui candidat pe luni întregi. Atacatorii care vă supraîncarcă site-ul web pot întrerupe comunicarea Dvs. cu susținătorii sau pot duce la donații pierdute în momentele cheie. Furtul datelor personale ale donatorilor sau ale alegătorilor duce la consecințe legale serioase, supune susținătorii Dvs. riscului de a fi hărțuiți și îi face pe donatori să ezite să doneze pentru campanie. Atacurile asupra calculatoarelor angajaților sau asupra serverelor campaniei pot întârzia operațiunile de campanie cu zile sau chiar cu săptămâni. Reabilitarea după un atac cibernetic va necesita resurse care sunt foarte prețioase în febra unei curse strânse, indiferent dacă este vorba de una prezidențială, parlamentară sau locală.

În viitorul apropiat, amenințările cibernetice vor rămâne o parte reală a procesului de campanie. În calitate de fruntași ai proceselor democratice, personalul de campanie trebuie să recunoască riscul unui atac, să elaboreze o strategie pentru a reduce cât mai mult acest risc și să implementeze strategii de răspuns în cazul în care un atac are loc. Deși nicio campanie nu poate obține o securitate perfectă, implementarea unor pași simpli poate crea dificultăți actorilor cu intenții rele. În mod ironic, cei mai sofisticați actori de stat aleg adesea cele mai simple metode de atac, concentrându-se pe persoanele și organizațiile care neglijează protocoalele elementare de securitate. Acesta este principalul motiv pentru care am creat acest manual.

În campaniile de astăzi, securitatea cibernetică este responsabilitatea tuturor. Erorile umane au fost, în mod constant, principala cauză a atacurilor cibernetice mediatizate și este rolul candidaților și liderilor de campanie să instituționalizeze conștientizarea securității în cultura organizației. Deciziile pe care le iau oamenii sunt la fel de importante ca software-ul pe care îl folosesc. În viitor, cele mai bune campanii vor avea standarde clare pentru munca grea, se vor menține de mesaj, vor fi loiale echipei și vor urma un bun protocol de securitate.

Înainte de a trece la recomandările noastre, haideți să formulăm problema:

- **mediul** în care se desfășoară campania Dvs;
- **amenințările** cu care s-ar putea confrunta campania Dvs; și,
- **importanța** gestionării riscurilor cibernetice.

Mediul Vulnerabil al Campaniei

La moment, campaniile sunt niște ținte deosebit de ușoare. Deseori, ele sunt temporare și tranzitorii. Ele nu dispun de timp sau bani pentru a dezvolta strategii de securitate pe termen lung și bine testate. Un număr mare de angajați se poate alătura echipei foarte repede, fără prea mult timp pentru instruiri. Ei își pot aduce propriul calculator de acasă—cu viruși în el! Mulți membri ai echipei de campanie trăiesc și lucrează la sute de kilometri distanță de sediul central. Lucrurile se mișcă rapid, mizele sunt adesea ridicate și oamenii simt că nu au timp să se gândească la securitatea informațională. Există o mulțime de oportunități pentru ca ceva să meargă greșit.

În același timp, campaniile se bazează din ce în ce mai mult pe informații personale despre alegători, donatori și opinia publică. Ele stochează documente sensibile, cum ar fi studii despre opoziție, studii de vulnerabilitate, liste de susținători, informația despre angajați, proiecte de politici publice și e-mailuri. Riscurile unui potențial atac sunt în creștere, la fel și consecințele.

PERICOLUL UNUI ATAC

Imaginați-vă acest scenariu: a rămas o lună până la ziua alegerilor și cursa este strânsă. Dvs. ajungeți devreme la sediu, luați o cafea sau ceai, ajungeți la biroul Dvs. și porniți calculatorul. Apare un ecran negru, apoi o caricatură a candidatului Dvs, urmată de un mesaj. Hard disk-urile Dvs. au fost șterse. Fiecare bit digital de informații pe care le-ați adunat—notițe strategice, liste de susținători, bilanțuri—nu mai există. Recuperarea acestei informații va costa un milion—sau renunțarea la o poziție politică majoră.

Un grup anonim a intrat în calculatorul Dvs. cu câteva luni în urmă și a furat în liniște e-mailuri, note strategice, adrese ale donatorilor și informație confidențială despre angajați. Grupul a petrecut săptămâni întregi căutând informație compromițătoare și distribuind momentele cheie pe rețelele de socializare și pe un website dedicat acestui lucru. Proeminent sunt prezentate informații dintro "carte de autoevaluare" a candidatului Dvs. Website-ul campaniei Dvs. a căzut, conturile din rețelele de socializare au fost suspendate pentru promovarea imaginilor indecente și nu există niciun calculator funcțional.

Amenințările întâmpinate de campanii

Din nefericire pentru campaniile și democrațiile din întreaga lume, adversarii interni și externi pot crede că prejudiciul sau ajutorul acordat unui anumit candidat servește interesele lor, fie că aceasta înseamnă crearea haosului și confuziei printre alegători, fie pedepsirea unui oficial care s-a pronunțat împotriva lor. Acest lucru poate părea rupt din cărțile de ficțiune, dar realitatea este că un serviciu de informații sofisticat, un criminal cibernetic sau un hacker pornit împotriva unui candidat v-ar putea alege pe Dvs. sau pe cineva din campania Dvs. drept țintă. Acestea sunt tipurile de amenințări posibile pe care managerii și personalul campaniei trebuie să le înțeleagă.

Pe măsură ce dezinformarea și campaniile de manipulare devin surse pentru inducerea în eroare a cetățenilor din întreaga lume, informația furată, scursă și interpretată poate duce la consecințe reale în alegeri. Mecanismele pe care le adoptați pentru protecția datelor și menținerea în siguranță a canalelor de comunicare sunt mai importante ca niciodată.

CINE SUNT HACKERII?

Campaniile se confruntă cu amenințări la adresa informațiilor și a securității cibernetice de la o gamă largă de actori. Hackerii "cu pălării negre" (“black hat” hackers) și infractorii cibernetici au încercat să compromită campanii din diverse motive: câștig personal, notorietate sau simpla dorință de a-și pune la încercare abilitățile. Țările străine reprezintă cea mai dedicată și persistentă amenințare. Grupurile de spionaj rusesc cunoscute sub numele de "Fancy Bear" (APT 28) și "Cozy Bear" (APT 29) au fost implicate în hack-urile de campanie din 2016 din SUA. Chinezii s-au concentrat mult mai mult pe colectarea informațiilor. Se crede că aceștia au fost activi în campaniile prezidențiale din 2008 și 2012 ale SUA, dar nu există dovezi că au scurs informații. Nord-coreenii s-au răzbunat pe compania Sony Pictures Entertainment pentru producția filmului “The Interview”: au furat și scurs emailurile companiei și au șters sistemele lor. În unele țări, campaniile opoziției sunt amenințate și de propriul guvern. Creșterea tensiunilor internaționale—în special în preajma alegerilor cu mize mari—ar putea provoca mai multe atacuri în viitor.

Gestionarea Riscurilor Cibernetice

Riscul este cel mai bine perceput prin trei componente. În primul rând, există vulnerabilități: slăbiciunile campaniei Dvs., care fac informațiile susceptibile la furt, modificare sau distrugere. Vulnerabilitățile pot apărea în hardware, software, procese și în nivelul de vigilență al personalului Dvs. Apoi, există amenințări reale: țări străine, hackeri și alte grupuri cu capacitatea de a exploata aceste vulnerabilități. Riscul apare atunci când există vulnerabilități și amenințări. În cele din urmă, există consecințe—impactul produs de actorii cu rea intenție care profită de riscurile care nu au fost adresate.

Dvs. sau campania Dvs. nu puteți face multe pentru a preveni amenințările în sine—ele sunt rezultatul unor forțe geopolitice, economice și sociale mai mari. Ceea ce puteți face, însă, este să reduceți substanțial posibilitatea succesului adversarilor Dvs., eliminând propriile vulnerabilități. Reducerea vulnerabilității reduce riscul—Dvs. decideți pe care le reduceți în mod prioritar. Bunăoară, ați putea decide că cel mai dăunator lucru pe care vi-l poate fura un hacker este raportului de autoanaliză a candidatului Dvs., așa că veți aloca resurse suplimentare pentru o stocare sigură online, care impune utilizarea parolelor lungi și restricționează accesul la un număr mic de persoane. Ați putea decide să securizați mai puțin unele documente de campanie și să le faceți disponibile pentru un număr mai mare de oameni, întrucât acestea sunt necesare angajaților și nu ar provoca daune prea mari în cazul unei scurgeri. Important este să rețineți că măsurile pentru securizarea datelor și prevenirea incidentelor cibernetice sunt supuse acelorași legi cu privire la protecția datelor care apar acum în toată lumea, cum ar fi Regulamentul General Privind Protecția Datelor (GDPR) în Europa.

Există aspecte tehnice de atenuare a riscurilor, specificate inclusiv în acest manual, însă cel mai mult contează abordarea Dvs. holistică. În calitate de lider al campaniei, cel mai important lucru pe care îl puteți face este luarea deciziilor fundamentale: cine are acces la informații, care informații sunt păstrate sau șterse, cât timp dedicați pentru instruiri, dar și propriul Dvs. comportament în calitate de exemplu. Ca profesionist în cadrul campaniei, gestionarea riscului este responsabilitatea Dvs.—atât din punct de vedere tehnic, cât și uman. Dvs. decideți care date și sisteme sunt cele mai valoroase și ce resurse dedicați pentru protecția lor.

Securizarea Campaniei

Recomandările noastre de securitate sunt organizate după trei principii:

1. Pregătiți-vă:

Succesul majorității recomandărilor din acest manual depinde de crearea, de către conducerea campaniei, a unei culturi de vigilență în domeniul securității, care minimizează punctele slabe. Aceasta înseamnă stabilirea unor reguli clare, care să fie impuse de sus în jos și respectate de jos în sus.

2. Protejați-vă:

Protecția este crucială. De obicei, atunci când descoperiți că aveți o problemă de securitate, este deja prea târziu. Construcția celei mai puternice protecții pe care puteți să v-o permiteți cu timpul și banii disponibili, este esențială pentru reducerea riscului. Securitatea online și protecția datelor funcționează cel mai bine în straturi: nu există o singură tehnologie sau produs universal de protecție. Combinând câteva măsuri de bază, puteți face arhitectura digitală a campaniei mai greu de pătruns și mai rezistentă, în cazul în care este compromisă, economisind astfel timp și bani pe care i-ați putea pierde în viitor.

3. Persistați:

Acum, adversarii campaniilor au tot mai multe resurse și expertiză; chiar și cea mai vigilentă cultură și cea mai dură infrastructură ar putea să nu fie capabile să împiedice o breșă de securitate. Campaniile trebuie să elaboreze din timp un plan pentru a face față unei eventuale breșe.

Unele campanii au mai mult timp și bani pentru securitatea cibernetică decât altele. De aceea, recomandările noastre oferă două niveluri de protecție: "bine" și "avansat". Nivelul "bine" reprezintă tot ceea ce trebuie să facă o campanie pentru a avea un nivel minim de securitate. Trebuie să aspirați mereu să faceți cât mai multe cu resursele de timp, bani și oameni de care dispuneți, de aceea vă recomandăm să utilizați nivelul "avansat" ori de câte ori este posibil. Dacă aveți resursele necesare pentru a achiziționa asistență IT specializată, veți face o investiție bună. Amenințările sunt într-o continuă evoluție, iar serviciile IT profesionale vă vor ajuta să depășiți ceea ce oferă acest manual și să fiți la curent cu cele mai recente amenințări și soluții pentru situația Dvs.

Managementul

Managerii de campanii trebuie să-și asume responsabilitatea pentru strategia de securitate cibernetică, însă majoritatea vor delega dezvoltarea și supravegherea acesteia unui director adjunct sau de operațiuni. Este important ca securitatea cibernetică să fie puternic integrată în resursele umane și tehnologia informațională, întrucât angajarea corectă a personalului, furnizarea hardware-ului și controlul permisiunilor de acces sunt esențiale pentru strategia Dvs. Multe campanii mici se bazează pe sprijinul voluntarilor în IT și securitatea cibernetică. Puteți folosi acest manual pentru a vă ghida discuția cu voluntarii. Este esențial să selectați minuțios voluntarii implicați și să controlați cu atenție accesul, astfel încât sprijinul voluntarilor să nu creeze noi vulnerabilități. Ar trebui să vă asigurați că cineva din personalul de campanie supraveghează munca în domeniul IT și controlează permisiunea de a accesa diferite sisteme.

Când să începeți?

Indiferent de modelul de suport pe care îl aveți, asigurarea securității cibernetice ar trebui să înceapă din prima zi. Ceea ce urmează este o listă de top cinci măsuri care sunt absolut vitale. Asigurați-vă că acestea există de la bun început, chiar dacă aveți doar unul sau doi angajați, apoi completați celelalte recomandări "bune" cât mai curând posibil. Dacă aceste măsuri nu au făcut parte din primul Dvs. plan digital, nu vă faceți griji. Nu este prea târziu să adoptați măsuri de securitate eficiente și să protejați ceea ce faceți deja.

Costurile

Multe măsuri recomandate în acest manual sunt gratuite sau au costuri foarte mici. De fapt, tot ce am inclus în lista noastră de top cinci este gratuit, cu excepția creării unei platforme online de stocare, care va costa doar câțiva dolari pe lună pentru fiecare angajat. Campaniile-țintă vor trebui să aloce resurse suficiente pentru hardware și software, pentru a executa o strategie responsabilă, însă aceste cheltuieli ar trebui să constituie un procent foarte mic din bugetul de mai multe milioane de dolari al campaniei. Campaniile mai mici vor putea implementa recomandările cu sume de la câteva sute până la câteva mii de dolari, în funcție de numărul de angajați sau de voluntari implicați în campanie.

Orice referință la furnizori și produse are drept scop să ofere exemple de soluții, dar nu este menită să influențeze alegerea Dvs. Dacă apar careva provocări atunci când folosiți produse sau servicii, vă încurajăm să contactați direct furnizorii, care de obicei vă pot oferi asistență tehnică. Când vine vorba de selectarea produselor și serviciilor, încurajăm fiecare campanie să consulte un expert în securitatea cibernetică sau să desfășoare cercetări independente pentru a găsi cel mai bun produs pentru nevoile lor.

Top Cinci Recomandări

1. 1. Stabiliți o cultură a conștientizării securității cibernetice:

Luați securitatea cibernetică în serios. Asumați-vă responsabilitatea pentru reducerea riscurilor, pregătiți personalul și voluntarii și setați exemplu. Factorul uman este cauza numărul unu a breșelor.

2. Utilizați o platformă de stocare online (cloud):

Un serviciu comercial mare de cloud va fi mult mai sigur decât orice ați puteți crea cu resurse limitate. Considerați utilizarea unei platforme complexe de stocare online, cum ar fi GSuite sau Microsoft365, care vă vor oferi toate opțiunile de bază de care ați putea avea nevoie și un loc sigur pentru stocarea informațiilor (a se vedea "Ce este cloud-ul" la pag. 18).

3. Utilizați autentificarea în doi factori și parole puternice:

Solicitați autentificarea în doi factori pentru a adăuga un al doilea nivel de protecție pentru toate conturile importante, inclusiv pentru platforma de lucru online, orice alt serviciu de e-mail sau de stocare și conturile Dvs. de pe rețelele de socializare. Utilizați o aplicație mobilă sau o cheie fizică pentru al doilea factor de autentificare, nu un SMS. Pentru parolele Dvs., creați CEVAFOARTELUNGCADEEXEMPLUACESTȘIR și nu ceva scurt de așa T1p. Contrar unei opinii des răspândite, un șir lung de cuvinte aleatorii fără simboluri este mai greu de spart decât ceva scurt, cu m@i mu1te $imb0lur!. Nu repetați niciodată parolele; un manager de parole vă poate ajuta și cu acest lucru, vă va permite să generați aleator parole puternice și va verifica parolele existente pentru a le identifica pe cele care au fost reutilizate.

4. Utilizați mesaje criptate pentru conversații și materiale sensibile:

Utilizarea unui instrument de mesagerie criptat pentru telefoane, ca Signal sau Wickr, pentru mesaje și documente sensibile nu va permite adversarilor să le obțină în caz că vă sparg cutia poștală electronică. Criptarea amestecă datele, reducând drastic probabilitatea ca cineva să vă poată citi mesajele, chiar dacă vă sunt interceptate datele.

5. Planificați și pregătiți-vă:

Elaborați un plan de rezervă în cazul în care securitatea Dvs. este compromisă. Stabiliți o persoană la care veți putea apela pentru ajutor tehnic, înțelegeți obligațiile Dvs. legale și fiți pregătiți să comunicați cât mai rapid și mai eficient posibil la nivel intern și extern.

Pași Pentru Securizarea Campaniei

Pasul 1: Factorul uman

Securitatea cibernetică este, întâi de toate, o problemă a factorului uman, nu una tehnică. Chiar și cele mai bune soluții tehnice nu vor produce efect dacă nu vor fi implementate corect sau dacă nu vor fi actualizate continuu odată cu dezvoltarea tehnologiei. Succesul măsurilor de securitate cibernetică depinde de crearea unei culturi a securității.

BINE — Ce trebuie să faceți

1. Stabiliți o cultură puternică a securității informaționale, care pune accentul pe securitate ca un standard pentru o campanie de succes. La fel cum sunt instruiți să nu încalce legile privind finanțarea campaniilor, angajații ar trebui să știe să evite accesarea link-urilor sau deschiderea atașamentelor în emailurile de la expeditori necunoscuți.

    a. **Inițierea:** Oferiți o instruire despre bazele securității informaționale pentru angajații noi. Puteți împărți materialele distributive în cadrul instruirii.

    b. **Instruiri:** Includeți subiectul securității informaționale în toate cursurile de formare continuă a personalului Dvs., cum ar fi evenimentele pentru membrii conducerii sau instruirile pre-electorale pentru mobilizare la vot (GOTV). Oferiți o pregătire suplimentară pentru cei care au roluri sensibile, cum ar fi candidatul, ofițerii de presă, personalul de conducere și oricine deține privilegii de administrator de sistem în rețeaua Dvs. Managerii ar trebui să solicite ca cei mai importanți oameni din campanie—inclusiv candidatul—să aibă setările de securitate verificate de responsabilul pentru IT (care poate fi însuși managerul). Nu ezitați să insistați asupra securității și față de candidat sau alte VIP-uri!

    c. **Setați exemplul:** Personalul de conducere al campaniei și candidatul trebuie să adopte un rol vizibil de leadership, promovând securitatea cibernetică în cadrul instruirilor. Ei trebuie să asigure o afirmare continuă a importanței securității cibernetice printre subalterni în cadrul întâlnirilor și al apelurilor. Nu lăsați doar pe seama experților tehnici să organizeze cursuri. Managerul de campanie sau directorul oprațional poate fi un mesager mai puternic, tocmai pentru că este considerat mai puțin "tehnic".

2. Verificați minuțios personalul, voluntarii și stagiarii—oricine solicită accesul la informațiile din campanie—pentru a evita acordarea acreditărilor unei persoane care dorește să fure date sau să vă saboteze sistemele.

a. Delimitați informația sensibilă și regulile pentru utilizarea acesteia. De exemplu, ați putea clasifica sondajele de opinie, rezultatele cercetărilor, documentele strategice și email-urile cu acest conținut drept “sensibile”.

b. Interziceți transferul de informații sensibile pe canalele de comunicare care nu sunt gestionate și securizate de campanie. Puteți cere ca acestea să fie transferate numai prin mesaje criptate (a se vedea Pasul 2).

3. Asigurați-vă că consultanții și furnizorii care au acces la informații sensibile au email și spațiu de stocare securizat (consultați Pasul 2). Când aveți îndoieli, solicitați furnizorilor și consultanților să utilizeze un cont pe platforma Dvs. de stocare online (consultați Pasul 2).

4. Controlați accesul la servicii online importante, cum ar fi conturile oficiale ale campaniei pe rețelele de socializare, pentru a împiedica folosirea lor de către persoane neautorizate. Asigurați-vă că cei care părăsesc campania nu mai pot accesa conturile legate de campanie. Puteți face acest lucru cu ușurință utilizând un instrument de gestionare a conturilor de pe rețelele de socializare care acționează ca o poartă către toate conturile Dvs. Dacă cineva părăsește campania, trebuie să-i dezactivați imediat contul.

5. Informați personalul despre amenințările de tip phishing (infracțiuni cibernetice). Asigurați-vă că știu cum să identifice și să evite link-urile suspecte și insistați pe importanța identificării și raportării potențialelor atacuri de acest tip. Ca parte a culturii puternice de securitate a campaniei, personalul de conducere ar trebui să-i laude pe toți cei care raportează un comportament suspect în sistemul lor sau recunosc că au accesat un link potențial rău intenționat.

6. Intrați în esența mediului legal în care operați. În anumite locuri, inclusiv în Uniunea Europeană, standardele de confidențialitate impun cerințe speciale pentru toate datele pe care le poate colecta campania Dvs., în special informațiile cu caracter personal, cum ar fi datele demografice sau adresa

Materiale distributive

» Pentru angajați
» Pentru membrii familiei

AVANSAT — Faceți următorul pas sledeći korak

7. Produsele software, cum ar fi Phishme și KnowBe4, vă pot instrui angajații prin transmiterea de emailuri de phishing false. Aceasta este o modalitate sigură, rapidă și eficientă de a identifica personele susceptibile accesării link-urilor suspicioase, astfel încât să le puteți oferi o instruire suplimentară. În același timp, multe dintre aceste produse filtrează unele încercări de phishing prin email.

8. Dacă dispuneți de resurse, angajați un specialist IT profesionist pentru a gestiona sistemele Dvs. de campanie și un expert în domeniul securității IT pentru a ajuta la protejarea, întreținerea și monitorizarea infrastructurii digitale a campaniei Dvs. Aceste persoane pot livra instruiri despre securitate, pot testa persoanele și sistemele Dvs. și vă pot personaliza soluțiile de securitate.

9. Încheiați un contract cu o companie de securitate cibernetică, care să vă furnizeze soluții de securitate, să revizuiască sistemul Dvs. de apărare și să monitorizeze sistemele în vederea identificării breșelor de securitate. Este important să cunoașteți care companie o veți contracta în cazul unei breșe de securitate și a necesității de asistență urgentă. Aceasta este o alternativă la angajarea unui expert în domeniul securității IT. Informați-vă în prealabil și selectați o companie cu o reputație bună—nu toate companiile de securitate cibernetică oferă același nivel de servicii.

LUCRUL CU SPECIALIȘTII ÎN SECURITATE

Dacă decideți să lucrați cu un profesionist în securitate, cum veți evalua persoana sau compania potrivită? Indiferent dacă este vorba de recomandări personale sau de recenzii pozitive, este important să evitați serviciile costisitoare dar ineficiente. Atunci când intervievați potențialii profesioniști în domeniul securității, întrebați-i cum au făcut față la incidentele de securitate anterioare și cum i-au ajutat pe alții să lucreze mai bine. Comitetul național al partidului Dvs. sau profesioniștii de încredere din campanie v-ar putea oferi recomandările necesare. Rețineți: cultura afectează securitatea, astfel chiar și cele mai bune recomandări pot să nu livreze rezultatele scontate dacă nu sunt respectate (doar angajarea unei companii nu vă va rezolva problemele).

Pasul 2: Comunicarea

Nu toate metodele de comunicare sunt la fel de sigure, deci trebuie să fiți extrem de atenți la modul în care comunicați. Conducerea campaniei ar trebui să stabilească un standard care să încurajeze conversațiile personale ori de câte ori este posibil și să descurajeze emailurile inutile. Orice ați scrie în email ar putea fi publicat în ziare sau pe rețelele de socializare—posibil cu unele modificări malițioase. Indiferent dacă este vorba de apeluri telefonice, trimitere de mesaje text sau expediere de email-uri, diferite produse și servicii oferă diferite niveluri de protecție, așa că faceți o alegere informată atunci când decideți ce sisteme veți utiliza în campanie.

BINE — Ce trebuie să faceți

1. Utilizați cele mai sigure sisteme posibile pentru comunicare.
    a. Utilizați servicii de mesagerie criptate de la utilizator la utilizator (end-to-end), cum ar fi Signal sau Wickr, în special pentru mesaje, trimiterea documentelor și apeluri telefonice. Multe campanii necesită transmiterea de informații sensibile numai prin mesaje criptate și este adesea mai ușor ca personalul din campanie să se obișnuiască să utilizeze aceste aplicații pentru toate comunicațiile de rutină (acest lucru este în special aplicabil pentru persoanele cu risc sporit, cum ar fi candidatul). Signal și Wickr publică codul sursă pentru verificare și oferă opțiuni care reduc riscul, cum ar fi posibilitatea de a șterge automat mesajele. Asigurați-vă că mesajele Dvs. nu se sincronizează cu calculatorul Dvs. sau cu conturile platformelor online de stocare.
    b. Dezactivați arhivarea serviciilor de mesagerie, cum ar fi Google Chat și Slack, astfel încât discuțiile vechi să nu poată fi scurse mai târziu. Acest lucru necesită intrarea în "setări" și ajustarea "politicilor de păstrare". Unele servicii vă cer să faceți acest lucru pentru fiecare conversație de chat. Vă recomandăm să păstrați mesajele de chat timp de o săptămână sau mai puțin.
2. 2. Utilizați o platformă de lucru online, care oferă comunicare prin email securizată, crearea documentelor online, chat și partajarea fișierelor, cum ar fi GSuite sau Microsoft365. De exemplu, GSuite include Google Drive pentru partajarea fișierelor, Gmail pentru crearea unei poște electronice, Google Hangouts pentru chat și Google Docs pentru procesarea de text, foi de calcul și prezentări. Microsoft365 oferă OneDrive / SharePoint pentru partajarea de fișiere, Outlook / Exchange pentru email, Microsoft Team pentru chat și Microsoft Office pentru procesare de text, foi de calcul și prezentări. În cazul în care nu intenționați să angajați profesioniști în securitate cu experiență (și potențial costisitori), platformele de lucru online gestionate de firmele majore vor fi mai bine protejate decât orice servere pe care le puteți configura în campania Dvs. Există versiuni gratuite ale celor două produse, însă versiunile plătite vă oferă mult mai multe capacități administrative. Google oferă, de asemenea, servicii gratuite pentru a proteja organizațiile

în medii periculoase, cum ar fi Outline, VPN; Project Shield, un serviciu care vă protejează site-ul împotriva atacurilor de dezactivare; și Password Alert, care vă avertizează când introduceți parola Gmail într-un site de phishing.

3. Ștergeți-vă email-ul

    a. Activați în aplicația de e-mail opțiunea “ștergerea automată” a e-mailurilor vechi, pentru a reduce numărul de e-mailuri care ar putea fi furate. De obicei, acest lucru necesită intrarea în setări și schimbarea "politicii de păstrare" pentru perioade mai scurte. Pentru a vă asigura că e-mailurile nu se află într-o mapă cu “articole șterse”, ajustați setările pentru a curăța automat acea mapă după o anumită perioadă. Vă recomandăm să păstrați e-mailurile timp de o lună sau mai puțin, cu excepția cazului în care este necesar din punct de vedere legal să le păstrați pentru perioade mai lungi. Ceea ce nu aveți, nu poate fi furat.

4. Securizați-vă conturile personale

    a. Chestiunile legate de campanie nu trebuie niciodată să ajungă pe conturile personale. Totuși, adversarii vor ținti să spargă conturile personale. Din acest motiv, angajații trebuie să folosească parole puternice și autentificarea cu doi factori inclusiv pentru conturile personale (acest lucru este inclus în materialul nostru distributiv pentru angajați).

CE ESTE CLOUD-UL?

Serviciile “Cloud” permit gestionarea și accesul la informațiile stocate la distanță pe Internet. Ele rulează pe servere la distanță administrate de companii terțe; aceasta includ multe servicii obișnuite pe care probabil le utilizați deja, cum ar fi Gmail sau Dropbox. Este bine să stocați informațiile la un furnizor de servicii cloud de încredere, nu pe calculatorul personal, deoarece acești furnizori au banii, resursele tehnice și expertiza necesară pentru a-și face serverele mai securizate decât hard disk-ul laptopului Dvs. sau un server de birou. Ei au, de asemenea, mult personal tehnic care lucrează pentru a preveni atacurile sofisticate asupra rețelelor lor (și, prin urmare, și asupra datelor Dvs.). O comparație apropiată ar fi alegerea de a păstra banii sub saltea, comparativ cu depozitarea lor în seiful unei bănci. Utilizarea serviciilor cloud oferă o protecție suplimentară împotriva pierderii de date, atunci când un dispozitiv individual este pierdut sau compromis. Stocarea în cloud este o funcție inclusă în serviciile de securitate de birou, cum ar fi GSuite și Microsoft365. Alte servicii includ Dropbox sau Box. Este important să rețineți că aceste corporații internaționale pot fi supuse cerințelor legale. Majoritatea corporațiilor majore, inclusiv cele menționate mai sus, au politici stricte pentru cazurile când se vor conforma unor astfel de cerințe.

ȘI DACĂ NU AM ÎNCREDERE ÎN CLOUD?

Unele organizații nu se simt confortabil cu ideea de a încredința informația lor unei companii terțe. Dacă insistați să vă administrați propria infrastructură tehnologică, fiți conștienți de faptul că va trebui să vă apărați împotriva forțelor de securitate ale țărilor străine. Iată câteva aspecte:

- Veți fi responsabil pentru înțelegerea, securizarea și remedierea tuturor aspectelor sistemelor Dvs., inclusiv a sistemelor de operare, aplicațiilor server, software-ului, bazelor de date și a tehnologiilor de conectare.
- Va trebui să vă asigurați că conexiunea la platformele Dvs. cheie este foarte fiabilă și nu este vulnerabilă la manipulare, cenzură sau DDOS (Distributed Denial of Service—paralizarea intenționată a unei rețele de calculatoare prin inundarea acesteia cu date trimise simultan de la mai multe calculatoare).
- Va trebui să monitorizați în mod activ tentativele de spargere și să aveți pe cineva de gardă 24/7.
- Va trebui să gestionați backup-uri securizate întro locație diferită.
- Dacă există pericolul unui raid fizic, toate informațiile Dvs. ar putea fi luate.

CE ESTE CRIPTAREA?

Criptarea este o modalitate de codificare a informației atunci când aceasta circulă între utilizatori, sau când este stocată, astfel încât aceasta să nu poată fi citită de nimeni în afară de destinatar. Gândiți-vă la proces așa: un utilizator "amestecă" datele atunci când le trimite și doar destinatarul are cheia pentru a le decodifica. Utilizarea criptării este un pas inteligent, mai ales pentru informații sensibile, deoarece chiar dacă un adversar fură datele, este puțin probabil că le va putea citi. Majoritatea aplicațiilor care utilizează criptarea, cum ar fi Signal sau Wickr, fac acest proces foarte simplu. Criptarea de la utilizator la utilizator (end-to-end) este o caracteristică importantă în programele de comunicații—înseamnă că mesajul Dvs. este secret până ajunge la destinație și nimeni—nici măcar furnizorul aplicației—nu poate citi mesajele. Dacă este posibil, utilizați și criptarea întregului disc pe laptop. Astfel, dacă acesta este furat sau uitat întrun autobuz, nimeni nu va putea citi conținutul.

CENZURA, SUPRAVEGHEREA ȘI DECONECTĂRILE DE LA INTERNET

Cu părere de rău, în multe părți ale lumii, tendințele de a stăpâni internetul (inițial conceput ca un spațiu deschis și democratic), sunt în creștere. Acestea pot include blocarea canalelor critice de comunicare, cum ar fi, de exemplu, WhatsApp sau Twitter; cenzura website-urilor publice sau să urmărească agresiv cetățenii care vă vizitează online și ce face personalul Dvs. în spațiul online. În cele mai grave situații, numărul cărora a crescut alarmant, o țară poate întrerupe în totalitate accesul la internet.

Aveți întotdeauna un plan de rezervă. Dacă partidul sau campania Dvs. depinde foarte mult de website-ul campaniei, asigurați-vă că pagina de Facebook are cele mai importante informații în cazul în care site-ul este blocat sau cenzurat. Dacă WhatsApp este un canal de comunicare de bază, fiți pregătit să utilizați SMS-ul sau să aveți un arbore telefonic de rezervă cu numerele tuturor. Dacă monitorizarea traficului web sau a activităților online ale personalului de campanie ar putea duce la probleme, considerați utilizarea unor instrumente de anonimizare, cum ar fi browserul Tor[1], Psiphon[2] sau VPN-ul Outline[3]. E bine să aveți la îndemână o listă a jurnaliștilor și, în cazul unor schimbări majore în cenzură sau întreruperi de internet, ajutați-i să facă din asta un reportaj.

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

PĂSTRAȚI SITE-URILE DVS. ONLINE

Site-ul campaniei Dvs. este probabil una dintre cele mai importante platforme publice de comunicare și una dintre cele mai ușoare căi prin care cetățenii vă pot găsi. Acest lucru face ca prezența Dvs. online sa fie o țintă deosebit de atractivă pentru hackerii rău intenționați sau rivalii fără scrupule. Considerați utilizarea unei platforme de găzduire cum ar fi Wordpress.com, Wix sau Google Pages, în care nu sunteți responsabil pentru administrarea website-ului. Dacă doriți să vă administrați propriul website, asigurați-vă că sunteți un expert sau că puteți angaja profesioniști pentru a-l apăra de hackeri.

Din ce în ce mai mult, atacatorii folosesc atacuri de tip DDOS pentru a doborî un website în perioadele critice, prin volume imense de cereri false. Rețelele de distribuție a conținutului (CDN) sunt capabile să mențină o copie “cache” a site-ului Dvs. pe servere puternice din întreaga lume, ceea ce face aproape imposibil ca toate să fie doborâte în același timp. Două produse care vă pot ajuta să protejați website-urile Dvs. publice sunt Cloudflare și Project Shield de la Google.

Pasul 3: Accesarea și Gestionarea Conturilor

Unul din cele mai dificile aspecte ale securității este protejarea de la accesări din partea persoanelor neautorizate. Aceasta înseamnă împiedicarea adversarilor să acceseze informația Dvs și împiedicarea accesului la informația de care oamenii din cadrul campaniei Dvs. nu au nevoie. Chiar dacă unele din recomandările de mai jos ar putea părea o povară, hackerii profită de cei care pun comoditatea mai presus de securitate.

CE ESTE AUTENTIFICAREA CU DOI FACTORI?

Autentificarea cu doi factori reprezintă un al doilea nivel de securitate care cere utilizatorului să furnizeze un credential în plus, în afară de parolă. Al doilea factor este esențial pentru că, dacă parola Dvs. este furată, adversarul oricum nu va putea accesa contul Dvs. Parola este ceva ce știți, iar al doilea factor este ceva ce aveți, ca de exemplu un cod generat de o aplicație, o cheie fizică sau chiar ceva biometric, ca o amprentă.

BINE — Ce trebuie să faceți

1. Solicitați autentificarea cu doi factori (2FA) pe toate sistemele și aplicațiile. Evitați să folosiți SMS-uri pentru autentificarea cu doi factori, deoarece atacatorii pot clona cu ușurință un număr de telefon și pot obține acces la SMS-uri. Există mai multe aplicații 2FA care funcționează la fel de bine ca și SMS-urile, cum ar fi Google Authenticator, Microsoft Authenticator și Duo Mobile. De asemenea, puteți utiliza o cheie fizică FIDO ("identitate rapidă online") pe care o inserați în drive-ul USB, cum ar fi Yubikey sau Feitian. Site-ul "TwoFactorAuth.org" este un ghid util pentru serviciile care oferă sau nu autentificarea cu doi factori.
2. Parole.
    a. Solicitați parole puternice. După cum am menționat mai devreme, "inventați parole lungi și puternice". Tehnologiile curente pot sparge o parolă de șapte caractere în câteva milisecunde. Un hacker va avea nevoie de mult mai mult timp pentru a sparge o parolă de 20 sau chiar 30 de caractere. Alegeți un șir de cuvinte pe care le veți memora ușor.
    b. Nu repetați parolele! Utilizați parole diferite pentru conturi diferite, astfel încât un hacker să nu poată sparge mai multe conturi dacă o singură parolă este furată.
    c. Pentru a proteja personalul campaniei și voluntarii împotriva atacurilor de tip phishing, transmiteți parolele față în față sau prin mesaje criptate de scurtă durată. Solicitați ca resetarea parolei pentru conturile centrale să fie cerută prin aceleași metode sau prin video

chat pentru a vă asigura că anume acel angajat sau voluntar al campaniei cere parola. Nu transmiteți niciodată parolele prin e-mail sau utilizând un sistem de asistență tehnică.

3. Utilizați un sistem de gestionare a parolelor, cum ar fi LastPass, 1Password sau Dashlane, pentru a gestiona cu ușurință multe parole lungi și puternice. Dar asigurați-vă că acest sistem de gestionare are o parolă lungă și puternică și dispune de autentificare cu doi factori. Nu recomandăm sisteme de gestionare a parolelor încorporate în browsere, cum ar fi Chrome, Safari și Firefox, pentru că acestea sunt deseori mai puțin sigure decât sistemele independente.

4. Creați conturi separate pentru administratori și utilizatori și restricționați atent accesul la conturile de administrator. Administratorii ar trebui să aibă două conturi separate—unul doar pentru administrare și altul care va fi contul standard folosit pentru toate celelalte activități de campanie. Acest lucru va reduce probabilitatea ca un adversar să poată compromite un cont de administrator, care ar oferi acces la întreaga rețea.

5. Periodic verificați cine are acces la diferite dispozitive și rețele. Blocați imediat accesul persoanelor care părăsesc campania. Schimbați imediat parolele dacă observați o activitate suspectă. Pentru a face posibil acest lucru, asigurați-vă că același cont de utilizator nu este folosit de mai mulți angajați.

MANAGERII DE PAROLE

Managerii de parole sunt o modalitate de a stoca, recupera și genera parole. Unele chiar pot popula automat câmpurile dedicate parolelor pe paginile de conectare. Managerii de parole necesită o parolă proprie pentru autentificare, care devine singura parolă pe care trebuie să o rețineți. Riscul, desigur, este că dacă cineva sparge acest sistem (s-a mai întâmplat), acea persoană va avea toate parolele Dvs. Dar acest risc este aproape întotdeauna depășit cu mult de avantajele pe care le oferă parolele puternice și unice pentru toate conturile Dvs. și riscul poate fi redus semnificativ prin utilizarea autentificării cu doi factori pentru managerii de parole. Pentru campanii, managerii de parole sunt utili pentru conturile care au mai mulți utilizatori, deoarece administratorul poate partaja în siguranță accesul la acestea.

AVANSAT — Faceți următorul pas sledeći korak

1. Creați conturi de utilizator pentru diferite tipuri de angajați ai campaniei, care acordă automat nivelul necesar de acces. Diferitele tipuri de angajați—voluntari, stagiari, personal de teren, conducerea campaniei—necesită acces la diferite resurse. Având conturi predeterminate, este mai ușor să vă asigurați că oamenii accesează doar ceea de ce au nevoie.

ŠTA SU ADMINISTRATORI?

U „informatičkom žargonu“, „administrator“ ili „admin“ može da ljudima omogući pristup ili kontrolu nad sistemima ili informacijama. Na primer, kao „admin“ za sistem elektronske pošte, možete kreirati naloge, menjati lozinke i postaviti uslove poput dužine lozinke i dvostepene autorizacije za sve naloge. U kancelarijskom programskom paketu kao što su GSuite ili Microsoft 365, takođe možete kreirati grupe kao što su „terenski tim“ ili „komunikacijski tim“. Posao admina je zaista važan. Ako sve urade kako treba, informacije će biti dostupne samo osobama kojima su potrebne, što je od suštinskog značaja za bezbednost. To znači da je odlučivanje o tome ko dobija administratorska ovlašćenja takođe odluka od kritične važnosti. Samo nekoliko obučenih osoba od velikog poverenja bi trebalo da drugima omogućava pristup informacijama. Ako član osoblja s „admin“ ovlašćenjima napusti kampanju, pobrinite se da im se odmah oduzmu ovlašćenja!

Pasul 4: Planificarea Răspunsului la Incidente

Planificarea răspunsului la un atac este la fel de importantă ca elaborarea unei strategii de securitate pentru a preveni un astfel de atac. Modul în care răspundeți afectează deseori rezultatul final al unui incident mai mult decât ceea ce a fost compromis. Trebuie să alocați timp pentru a discuta cu liderii sau managerii ce veți face în momentul în care ceva se va întâmpla. Iată o listă a pașilor pe care ar trebui să îi faceți:

LEGALI

Identificați pe cineva din exterior, pe pare îi puteți contacta în cazul unui atac cibernetic. Discutați cu ei procesul de reacție la începutul campaniei. În cele mai multe cazuri, va fi aceeași persoană care reprezintă campania Dvs. cu privire la alte chestiuni, dar în mod ideal ar trebui să aveți pe cineva care este specializat în răspunsul la astfel de incidente.

Rugați avocatul Dvs. să vă explice obligațiile legale în cazul în care datele sunt furate și ce măsuri de rigoare trebuie să pregătiți.

Înțelegeți care sunt obligațiile legale ale furnizorilor de a vă notifica pe Dvs. sau pe alții atunci când sunteți atacați. Ori de câte ori este posibil, includeți cerințe stricte de notificare în contractele cu furnizorii, deoarece părțile terțe reprezintă o sursă frecventă de atac.

Dacă credeți că ați fost atacat, o bună practică este ca avocatul să gestioneze răspunsul Dvs. sub privilegiul avocat-client.

Discutați cu avocatul Dvs. despre cea mai bună modalitate de a colabora cu autoritățile în cazul unui atac. Fiecare campanie va aborda acest lucru în mod diferit.

TEHNICI

Determinați din timp la cine veți apela pentru a solicita asistență tehnică atunci când veți suspecta că ați fost atacat.

Alegeți pe cineva din campanie care va interacționa cu experții tehnici în cazul unui atac. În mod ideal, ar trebui să fie aceeași persoană care coordonează deja partea tehnică a campaniei. Gestionarea răspunsului la un incident poate fi copleșitoare, deci aveți nevoie de cineva care să se concentreze asupra aspectelor tehnice și care știe ce face. Astfel, vă veți puteți concentra pe comunicarea cu părțile interesate și cu presa.

Aflați mai multe despre asistența tehnică sau despre alt suport pe care furnizorii de platforme pot să vi-l ofere în cazul unui incident cibernetic.

OPERAȚIONALI

Decideți din timp cine va face parte din echipa Dvs. de intervenție în caz de incidente și cine va participa la ședințele de redresare a incidentelor. Este important să includeți pe cineva din echipele IT, legale, de operațiuni și de comunicare. Dacă sunteți o campanie mică și nu aveți persoane responsabile doar de comunicare, IT sau operațiuni, planificați să includeți orice persoane cheie care supraveghează operațiunile de campanie.

Determinați lanțul de luare a deciziilor în cazul unui incident, în special în ceea ce privește comunicațiile. În multe cazuri, acesta va fi managerul de campanie, dar unii manageri pot alege să delege responsabilitatea altcuiva.

Identificați ce aplicație sau tehnologie veți utiliza pentru a comunica dacă credeți că sistemele Dvs. au fost atacate. De exemplu, dacă e-mailul Dvs. este compromis, vă recomandăm să vă bazați pe o aplicație de mesagerie securizată, cum ar fi Signal sau Wickr. Comunicarea în timpul unui atac este esențială, dar Dvs. nu doriți ca adversarii să știe ce discutați—sau că răspundeți la acțiunile lor.

COMUNICAȚII

Planificați pentru diferite scenarii. Pentru multe campanii, acest lucru poate face parte din strategia existentă. Pentru campanii mari, unde riscurile sunt mai mari, ar putea fi necesară o ședință separată.

Identificați actorii cheie interesați, interni și externi, cum ar fi personalul campaniei, voluntarii, donatorii și suporterii. Trebuie să știți pe cine să contactați dacă apare un incident și trebuie să îi clasați în ordinea priorității. Elaborați o listă de persoane care trebuie contacte și delegați pe cineva care îi va contacta.

Faceți o listă cu de cele mai dăunătoare scenarii și gândiți-vă cum actorii interesați și mesajele Dvs. se pot schimba pentru fiecare din ele. Scenariile ar putea include:

- Zvonuri că a fost atacată campania Dvs;
- Scurgeri de informații personale despre susținători;
- Furtul de informații financiare sensibile despre donatori, cum ar fi numerele cărților de credit și date de contact;
- Vi se cere recompensă pentru recuperarea datelor furate;
- Sistemele Dvs. au fost șterse și închise;
- Email-urile cuiva au fost furate;

- Adversarul Dvs. a furat credențialele administratorului și toate fișierele stocate pe drive-ul campaniei;
- Conturile Dvs. de pe rețelele de socializare sunt șterse sau sparte de hackeri;
- Internetul este deconectat, sau anumite pagini web, aplicații sau protocoale sunt blocate la nivel național;
- Accesul la informație critică este blocat sau întrerupt prin cenzură.

Aveți grijă ce spuneți despre politicile pe securitatea cibernetică sau incidente cibernetice. Unele victime ale crimelor cibernetice au făcut anterior declarații grandioase despre propriile lor măsuri de securitate, sau i-au criticat pe alții care au fost atacați. Presa vă va taxa pentru ceea ce ați spus în trecut, dacă deveniți victime.

La fel, evitați să oferiți detalii despre amploarea evenimentului în primele faze ale incidentului (dacă puteți să evitați în general să discutați amploarea, cu atât mai bine). Detaliile disponibile la început se vor schimba pe parcursul investigației. O greșeală des întâlnită este să spuneți ceva, care mai târziu se va adeveri a fi fals (e.g., "ei nu au furat foarte mult," sau "niciun fel de informație personală nu a fost furată"). Calea cea mai sigură este să spuneți doar ceea ce știți cu siguranță. Declarațiile ar trebui să se axeze pe acțiunile pe care le întreprindeți pentru a corecta situația pentru actorii implicați care au fost afectați.

Elaborați din timp un fel de limbaj șablon, în mod ideal în consultație cu reprezentanții voștri legali, astfel încât să puteți elabora declarații sau repere de discuție repede, în caz că are loc un incident. Minimul pe care îl puteți face este să creați un document simplu cu întrebări și răspunsuri pe care îl puteți revizui rapid în caz că trebuie să îl folosiți. Crearea din timp a unui document cu întrebări și răspunsuri vă va ajuta să vă gândiți nu doar la ce veți spune, dar și ce nu veți spune. De exemplu, deseori, prima întrebare va fi "Ce s-a întâmplat?" Totuși, s-ar putea întâmpla ca Dvs. să nu puteți răspunde la această întrebare timp de câteva zile, sau chiar săptămâni. Faptul că nu știți ce fel de atac va avea loc, poate chiar să vă ajute să elaborați din timp niște răspunsuri mai bune.

ÎNTEBĂRI PE CARE SĂ LE INCLUDEȚI ÎN DOCUMENTUL CU ÎNTREBĂRI ȘI RĂSPUNSURI:

- Ce s-a întâmplat?
- Cum s-a întâmplat?
- Cine a făcut acest lucru?
- Ceva a fost furat sau afectat?
- A fost furată informația personală a cuiva? Ce faceți pentru a-i proteja?
- Cum au făcut asta hackerii?
- Hackerii au ieșit din sistemul Dvs.?
- Cât timp au stat ei în sistemul Dvs.?
- Ce măsuri de securitate foloseați? De ce nu au fost eficiente?
- Nu ar fi trebuit să știți că acest lucru se va întâmpla? De ce sistemele Dvs. nu erau mai bine securizate?
- Lucrați cu organele de drept? Ați fost contactați de aceste organe?
- În cazul unui atac unde se cere recompensă, veți fi întrebați: Ați plătit recompensa? De ce, sau de ce nu?

Păstrați legătura cu actorii cheie implicați și oferiți-le cât mai multă informație. Probabil nu veți putea să spuneți multe, dar este crucial să îi contactați în mod regulat, spunându-le ceea ce știți, să aveți o declarație clară despre intențiile Dvs. și să oferiți detalii despre ce faceți pentru a gestiona situația. Evitați să creați așteptări de contacte prea frecvente, pentru că deseori nu veți avea informație nouă și actorii implicați vor deveni frustrați dacă continuați să reveniți la ei fără informații noi. Vorbiți proactiv cu mass-media doar dacă aveți informații noi de oferit.

Pasul 5: Dispozitive

Fiecare dispozitiv fizic în campania Dvs.—de la telefon mobil, tabletă sau laptop, până la router, printer sau aparat foto/video—reprezintă o cale potențială de atac în rețeaua Dvs. Un plan bun de siguranță cibernetică va încerca să controleze accesul în, la și de la toate dispozitivele. Puteți controla accesul la dispozitive asigurându-vă că acestea sunt mereu folosite corect și știți cui aparțin. Controlați accesul în dispozitive prin autentificarea cu doi factori și parole puternice. Controlați conținutul dispozitivelor prin criptare și prin politicile care reglementează stocarea informației (i.e., stocarea informației pe cloud, în loc de dispozitive).

BINE — Ce trebuie să faceți

2. Utilizați mereu ultima versiune disponibilă a sistemului de operare, deoarece actualizările includ mereu patch-uri pentru ultimele vulnerabilități. Dacă este posibil, setați dispozitivele să instaleze automat aceste actualizări. Numiți o persoană responsabilă de verificarea sistematică a actualizărilor.

3. Faceți backup! Pentru orice informație pe care o păstrați pe un dispozitiv local (de exemplu, calculatorul Dvs.), asigurați-vă că aveți un plan de backup, în caz că calculatorul este furat, se strică, sau vărsați cafea peste tastatură. De exemplu, puteți folosi un serviciu automat de backup pe cloud pentru a mitiga impactul pierderii informației. Exemple includ Backblaze și CrashPlan.

4. Accesul la dispozitiv

    a. Încă de la început, cei care conduc campania ar trebui să creeze un mediu în care oamenii iau în serios securitatea fizică a dispozitivelor lor—pierderea unui dispozitiv ar putea da adversarilor acces la informație critică pe care o pot folosi pentru a dăuna campaniei Dvs.

    b. Deși multe campanii nu își pot permite să cumpere dispozitive noi, mereu este mai bine să cumpărați echipament nou (în special calculatoare și telefoane), dacă puteți. Minimul pe care îl puteți face este să oferiți dispozitive noi personalului care operează cu informație sensibilă, sau cel puțin să ștergeți și să reinstalați sistemul de operare pe dispozitivele vechi. Dacă angajații folosesc calculatoarele și telefoanele personale, stabiliți o politică de folosire a dispozitivelor personale prin care să implementați practici puternice de securitate (vedeți protecția endpoint mai jos).

    c. Membrii campaniei NU trebuie să folosească conturi personale de email sau dispozitive care nu au fost securizate conform procedurii de folosire a dispozitivelor personale pentru chestiuni legate de campanie, inclusiv email și rețele de socializare. Orice informație importantă care se găsește în afara dispozitivelor sau sistemelor controlate de campanie

este vulnerabilă la atacuri. Conducerea ar trebui să insiste sistematic ca informația legată de campanie să fie ținută separat de conturile personale de email sau calculatoare nesecurizate.

d. Mențineți securitatea fizică a dispozitivelor Dvs. Când sunteți în transport public, cafenele sau chiar în oficiu, mereu luați măsuri împotriva furtului dispozitivelor care ar putea oferi acces la conturile, comunicarea și informația Dvs.

e. Raportați imediat dispozitivele pierdute. Cereți setările care permit ștergerea de la distanță a informației aflate în toate dispozitivele. Exemple includ opțiunile “Find my iPhone” și “Android Device Manager”.

f. Fie că pierdeți sau câștigați, stabiliți un plan pentru ce se va întâmpla cu toată informația, conturile și dispozitivele atunci când campania se va încheia. Perioada imediat următoare după campanie este o perioadă deosebit de vulnerabilă.

5. Accesul în dispozitive

a. Schimbați parolele și setările implicite pentru toate dispozitivele. Multe dispozitive au parole setate din fabrică care sunt foarte ușor de ghicit. Dezactivați contul de oaspete la dispozitivele care au astfel de setări.

b. Activați opțiunea “auto-lock” (blocare automată) pentru telefoane și calculatoare după 2 minute de inactivitate și solicitați o parolă sau amprentă pentru deblocare.

c. Activați opțiunea “auto-wipe” (ștergere automată) pentru telefoane, astfel încât ele să șteargă informația după un număr anumit de încercări eșuate de accesare.

6. Conținutul dispozitivelor

a. Solicitați criptarea pentru toate dispozitivele (calculatoare și telefoane) pentru a vă asigura că pierderea unui dispozitiv nu va compromite informația aflată în el. Exemple includ: FileVault pentru Mac și BitLocker pentru Windows. Unele dispozitive ca iPhone fac acest lucru automat, dar nu toate.

b. Instalați software de protecție a punctului final (endpoint protection software) pe toate dispozitivele. Unele exemple includ Trend Micro, Sophos și Windows Defender. Există aplicații speciale de securitate endpoint pentru telefoane și tablete, ca de exemplu Lookout.

CE ESTE PROTECȚIA ENDPOINT?

Endpoints sunt dispozitivele folosite de membrii echipei, inclusiv telefoane mobile, laptopuri și calculatoare. Ele sunt “punctele de final” ale rețelei campaniei, și membrii echipei sunt “utilizatorii finali.” Protecția endpoint în mod centralizat controlează și gestionează securitatea pe dispozitivele la distanță. Este extrem de importantă mai ales pentru campaniile care permit membrilor echipei să folosească dispozitivele personale, deoarece campania trebuie să asigure că dispozitivul este securizat, fără viruși și poate fi șters în caz de furt sau pierdere. Protecția endpoint de asemenea poate monitoriza dispozitivul pentru a se asigura să software-ul este actualizat și poate detecta viruși sau potențiale amenințări de securitate. Pentru multe campanii, acesta va părea un pas mare, dar includerea acestei protecții în rutina Dvs. și investiția de timp vă poate scăpa de multe probleme ulterioare.

AVANSAT — Faceți următorul pas sledeći korak

1. Folosiți software de gestionare a dispozitivelor mobile, care monitorizează activitatea pentru a vă asigura că toate dispozitivele se conformează politicilor de securitate stabilite pentru telefoane mobile și alte dispozitive. Exemple includ VMware AirWatch, Microsoft InTune, și JAMF. GSuite și Microsoft Office 365 de asemenea includ un serviciu de gestionare a dispozitivelor mobile.

2. Utilizați servicii avansate de protecție împotriva amenințărilor, care monitorizează și vă alertează la detectarea activității rău intenționate, ca CrowdStrike Falcon sau Mandiant FireEye. Crowdstrike uneori oferă serviciul Falcon de prevenire a breșelor pro bono prin Crowdstrike Foundation, în dependență de necesitățile campaniei Dvs. și de regulile de finanțare a campaniei.

Pasul 6: Rețele

Rețelele sunt alcătuite din sistemul de echipament fizic (hardware), software digital și conexiunile între ele. Rețelele reprezintă alt mediu larg deschis pentru atacuri. Securitatea rețelelor cuprinde totul, de la cum dispozitivele comunică între ele, până la folosirea serviciilor cloud pentru stocarea informației.

BINE — Ce trebuie să faceți

1. Stocați informația pe servicii cloud de încredere, nu pe calculatoare sau servere personale. Orice informație stocată pe un dispozitiv personal este supusă unui risc mai mare de furt, accident și atacuri din partea hackerilor, decât informația stocată pe cloud.
    a. Nimeni nu ar trebui să aibă acces la toate fișierele din rețea; conturile cu acces comprehensiv de administrator nu trebuie folosite pentru lucrul de zi cu zi. Împărțiți stocarea fișierelor în mape pe departamente și oferiți acces corespunzător.
    b. Asigurați-vă că accesul la conținutul partajat cu alții este posibil doar prin invitații. Unele servicii de gestiune a fișierelor permit și includerea unui termen de expirare pentru invitații și acces.
    c. Periodic, organizați un audit al tuturor fișierelor care sunt partajate și a persoanelor care au acces la ele.
2. Creați o rețea wifi separată pentru vizitatori și voluntari, care limitează accesul lor la resursele campaniei. Încercați să cumpărați routere care oferă un "profil pentru oaspeți", care va segmenta automat rețeaua Dvs. Vă încurajăm insistent să schimbați parola pentru rețea la sfârșitul campaniei, când mulți angajați se vor schimba sau vor pleca.
3. Când călătoriți, sau înainte de a amenaja oficiul campaniei, evitați cât mai mult posibil rețelele wifi publice și utilizați doar rețele de încredere. Dacă aveți nevoie de wifi mobil, încercați să oferiți staffului de campanie hotspoturi wifi mobile. Wifi-ul public este deseori gratis și este foarte ușor de conectat la el, dar atacatorii de asemenea îl pot folosi pentru a pătrunde în echipamentul Dvs. fizic (hardware).
    a. Pe cât posibil, stafful ar trebui să folosească un VPN (rețea virtuală privată). VPN-urile ajută la protejarea împotriva intrușilor când sunteți conectați la un wifi public. Exemple de servicii VPN includ ExpressVPN sau TunnelBear. Nu toate VPN-urile sunt create la fel. Aveți grijă la serviciile gratis: multe dintre ele doresc să vă ia datele!
4. Securizați-vă browserul. PC Magazine a clasat Chrome și Firefox ca cele mai sigure browsere în 2017. Indiferent de ce browser folosiți, păstrați-l actualizat.

CE SUNT VPN-URILE?

O rețea virtuală privată (VPN) este un "tunel" criptat pentru traficul Dvs. de internet, care îl ascunde de intruși. Unele oficii îl folosesc ca o metodă de a se autentifica de la distanță în rețeaua oficiului, dar acest lucru nu este foarte obișnuit pentru campanii. Campaniile ar trebui să considere opțiunea de a încuraja stafful să folosească un VPN pe calculatoare și telefoane mobile dacă folosesc deseori wifi public sau rețele în care nu au încredere (lucru relevant pentru stafful care călătorește mult, sau pentru oficiile din teritoriu). Google recent a lansat un nou sistem, numit Outline, care permite crearea propriului VPN.

AVANSAT — Faceți următorul pas sledeći korak

1. Puteți lua măsuri mai avansate pentru a proteja rețeaua Dvs, dar ele ar trebui implementate de un profesionist în domeniul IT. Noi vă sugerăm să îi cereți să includă următoarele:
    a. Să configureze un hardware firewall.
    b. Să cripteze conexiunea Dvs. wifi folosind protocolul de securitate WPA2 sau 802.1x (nu folosiți WEP).
    c. Să configureze proxy-uri web bazate pe cloud, pentru a bloca accesul la website-uri suspicioase de la orice dispozitiv deținut de campanie, indiferent de locația acestuia. Exemple de furnizori de astfel de servicii includ Zscaler, Cisco Umbrella și McAfee Web Gateway Cloud Service.
    d. Stocați înregistrarea activității Dvs. (activity log) pe un furnizor de servicii cloud precum LogEntries sau SumoLogic.
    e. Segmentați stocarea Dvs. pe cloud, astfel încât nu toată informația să fie stocată în același loc. Studiile referitoare la opoziție, documentele strategice și fișierele personalului trebuie păstrate în mape diferite, iar accesul la acele mape ar trebui restricționat și oferit doar acelor persoane care întradevăr au nevoie de ele. Considerați opțiunea de a avea în general un sistem de stocare diferit pentru cea mai sensibilă informație a campaniei. Restricționați accesul, astfel încât doar câțiva oameni cheie să o poată accesa, și doar folosind anumite dispozitive. (De exemplu, dacă folosiți Microsoft365 pentru stocarea documentelor, puneți cele mai sensibile documente întrun cont Dropbox sau Box.) Dacă un membru al campaniei devine compromis, acest tip de segmentare poate limita daunele.
2. Instruiți stafful să nu conecteze dispozitivele lor la porturi sau dispozitive necunoscute. Nu folosiți încărcătoare publice în aeroport sau la evenimente. Nu acceptați încărcătoare pentru telefon sau baterii gratis la evenimente (acel stick USB poate fi plin de viruși!).

Pasul 7: Operațiunile Informaționale și Comunicarea cu Publicul

Operațiunile informaționale recent au apărut destul de des în știri, în special campaniile serviciilor externe de informații. Politicienii și oamenii care elaborează politici publice sunt cei care vor trebui să decidă cum să lupte cu operațiunile informaționale de acum înainte, iar noi, ca staff de campanie, nu putem face multe pentru a influența dacă ele au loc sau nu. Totuși, sunt câteva lucruri pe care le putem face pentru a le gestiona, dacă au loc. Campaniile au fost, și vor continua să fie, ținte ale acestor operațiuni, și trebuie să fim pregătiți. Apărarea modului în care campania Dvs. comunică cu publicul este importantă. Mai jos sunt câteva moduri de a vă proteja mai bine împotriva operațiunilor informaționale, de a identifica când acestea se întâmplă campaniei sau candidatului Dvs, și cum să răspundeți rapid când ele au loc.

CE SUNT OPERAȚIUNILE INFORMAȚIONALE?

Informația este putere—sau cel puțin asta susțin mulți militari și serviciile de informație! Puterea ideilor deja de mult timp alimentează răscoalele, insurecțiile și războaiele civile. Multe țări care au capacități militare inferioare, în sensul tradițional, caută să folosească informația pentru a diviza și preocupa adversarii lor. În Rusia, de exemplu, influențarea opiniei publice prin propagandă și alimentarea tensiunilor locale este parte a doctrinei lor de război și ceva ce ei practică constant asupra adversarilor. Rețelele de socializare au schimbat complet jocul operațiunilor informaționale. Acum, informația poate fi mișcată mai repede și oamenii sunt mai ușor de impresionat ca niciodată, creând impresia furiei publice sau a divizării.

BINE — Ce trebuie să faceți

3. Rețineți: operațiunile informaționale sunt o problemă de comunicare, nu una tehnică. Adversarii pot face operațiunile lor informaționale mai convingătoare furând informația voastră, dar odată ce informația ajunge publică, aveți nevoie de o strategie de comunicare pentru a o gestiona. Gândiți-vă din timp cum veți trata știrile false sau eronate—o să le ignorați? O să le dați share și o să susțineți că sunt false? Cum veți lua această decizie? Acestea sunt printre cele mai dificile decizii pe care trebuie să le adopte o campanie, dar

ceea ce contează cel mai mult este să vă gândiți din timp la aceste întrebări, împreună cu echipa, ca să aveți o strategie cum să reacționați, dacă decideți să reacționați.

4. Fiți la curent cu ce se întâmplă. Încurajați activiștii să se împartă cu postări, website-uri sau știri care le par suspicioase. Dacă doriți, puteți delega unii voluntari să se concentreze anume pe acest lucru, să caute ce fel de conținut este publicat. Totuși, este imposibil să cunoașteți toată informația pe care alegătorii pot să o vadă pe Facebook. Platforma a făcut mai dificilă postarea reclamelor politice și a mărit numărul de angajați care monitorizează conținutul știrilor, dar este imposibil de verificat toate postările. Cel mai bun mod de a rezolva această problemă la moment este să delegați o echipă de voluntari, din diferite categorii demografice și geografice, astfel încât să reușiți să găsiți cât mai multe postări de acest fel.

5. Stabiliți contacte cu platformele principalelor rețelele de socializare și anunțați-le dacă descoperiți informație falsă. Majoritatea platformelor rețelelor de socializare acum șterg conținutul "fals" sau care duce electoratul în eroare, precum și profilele false. Rugați comitetul campaniei sau partidul central să vă dea contactele acestor platforme și stabiliți o legătură cu ele la începutul campaniei, astfel încât să îi puteți contacta repede atunci când se întâmplă ceva.

    a. Facebook

    b. Twitter

    c. Google/Youtube

6. Monitorizați siteurile impostoare. La moment, nu există rapoarte publice despre impostori care încearcă să fure bani sau informație despre activiști prin website-uri false, dar acesta este un vector de atac foarte ușor, iar Dvs. ar trebui să fiți vigilenți. Cumpărați orice adresă web pe care ați vrea să o folosiți (sau care ar putea fi folosită împotriva Dvs.). Dacă doriți, puteți menține un serviciu de gestiunare a reputației, care va monitoriza spațiul web pentru Dvs. Uneori acest lucru poate fi făcut la un preț destul de modest.

7. Protejați-vă de un atac DDoS. Un atac DDoS are loc atunci când un adversar obține controlul multor dispozitive și le folosește pentru a "bombarda" în același timp website-ul Dvs., ducând la căderea acestuia. Majoritatea lucrurilor pe care ne-am concentrat în acest manual au fost despre cum să țineți oamenii departe de informația Dvs. despre campanie, dar în cazul unui DDoS, Dvs. vreți să păstrați website-ul deschis și disponibil mereu pentru donatori și activiști. DDoS încă nu a devenit o amenințare des întâlnită pentru campanii, dar ar putea fi folosit pentru a vă împiedica să colectați fonduri sau pur și simplu să creeze o perturbare destul de frustrantă a camaniei Dvs. Există două instrumente gratuite pe care le puteți folosi pentru a vă proteja website-ul: Google Shield și Cloudflare.

Aveți idei pentru îmbunătățirea acestui manual?

Există tehnologii sau vulnerabilități noi pe care ar trebui să le abordăm?

Așteptăm părerea Dvs.

Vă rugăm să ne împărtășiți ideile, istoriile și comentariile Dvs. pe Twitter @d3p folosind hashtag-ul #CyberPlaybook sau să ne trimiteți un e-mail la adresa connect@d3p.org, pentru a continua îmbunătățirea acestui manual pe măsură ce mediul digital se schimbă.

Protejarea Democrației Digitale
Centrul Belfer de Știință și Relații Internaționale
Școala de guvernare John F. Kennedy
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Copyright 2018, President and Fellows of Harvard College

Imaginile folosite aparțin proiectului Noto Emoji, licențiat de Apache 2.0