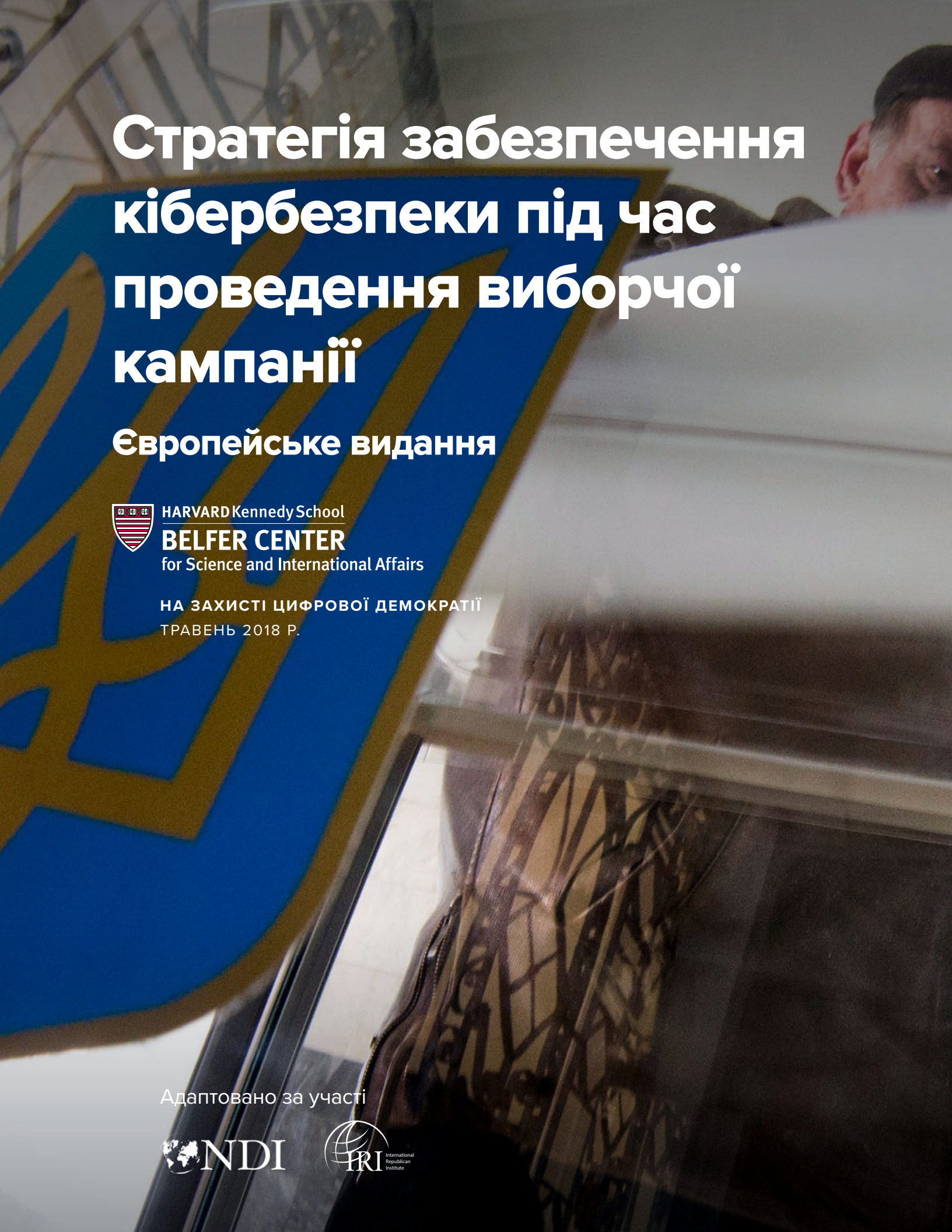


Стратегія забезпечення кібербезпеки під час проведення виборчої кампанії

Європейське видання

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

НА ЗАХИСТІ ЦИФРОВОЇ ДЕМОКРАТІЇ

ТРАВЕНЬ 2018 Р.

Адаптовано за участі

NDI IRI International Republican Institute

Defending Digital Democracy Project
Проект «На захисті цифрової демократії»

Центр «Белфер» з питань науки та міжнародних справ
Школа управління імені Джона Ф. Кеннеді

79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Партнери європейської версії:

Національний Демократичний Інститут
www.ndi.org

Міжнародний Республіканський Інститут
www.iri.org

Дизайн та макет – Ендрю Фасіні (Andrew Facini)

Фото на обкладинці: Чоловік кидає свій виборчий бюлетень під час парламентських виборів на виборчій дільниці у Волновахе в неділю, 26 жовтня 2014 р. (AP Photo/Dmitry Lovetsky)

Стратегія забезпечення кібербезпеки під час проведення виборчої кампанії

Європейське видання

Зміст

Вітальне слово

Люди беруть участь у виборчих кампаніях з різних причин: обрання лідера, в якого вони вірять, просування порядку денного, очищення влади, або заради «кайфу» та адреналіну під час кампанії. Це – деякі з причин, що приводять нас до політики. Ми точно не прийшли до неї тому, що хотіли стати кіберекспертами, і думаємо, що ви також.

На жаль, кіберзагрози зростають та мають спроможність повністю розвалити вашу кампанію. Ми займаємося кампаніями та підтримкою міжнародних демократичних процесів, і ми бачили на власні очі, як хакерство, дезінформація та видалення веб-сайтів можуть вплинути на перебіг виборів, а також на вектор країни.

D3P – це двопартійна команда державних та приватних експертів з кібербезпеки, а також експертів з великим досвідом проведення політичних кампаній. У цьому виданні ми працювали у партнерстві з Міжнародним Республіканським Інститутом (IRI) та Національним Демократичним Інститутом (NDI) для кращого розуміння виборчого контексту та як враховувати кібер-ризики та захищатися від них.

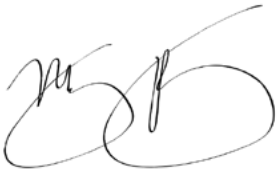
Ми належим до різних політичних партій та не багато у чому погоджуємося, коли йдеться про державну політику, але є одна річ, яка нас об'єднує – це віра у те, що саме виборці мають приймати рішення на виборах, і ніхто інший. Все більш цифровий спосіб нашого життя та роботи надає нові можливості для опонентів впливати на нашу кампанію та на вибори. Хоча вам й не треба бути кіберекспертом для того, щоб успішно провести кампанію, ви несете відповідальність за захист свого кандидата та партії від опонентів у цифровому просторі. Саме тому у рамках проекту «На захисті цифрової демократії» Центру «Белфер» з питань науки та міжнародних справ Школи управління ім. Джона Ф. Кеннеді було створено цю **Стратегію забезпечення кібербезпеки під час кампанії** [PDF].

Національний Демократичний Інститут, Міжнародний Республіканський Інститут та десятки обраних посадовців, експертів з безпеки та професійних керівників виборчих штабів співпрацювали з проектом «На захисті цифрової демократії» для адаптації цієї Стратегії до ширшого міжнародного контексту.

Інформація, зібрана тут, підходить для будь-якої кампанії у будь-якій партії. Вона має на меті озброїти вас простими та дієвими способами захистити інформацію вашої кампанії від опонентів, які намагаються атакувати вашу партію та демократію у вашій країні. Понад усе ми сподіваємось, що цей ресурс дозволить вам витрачати більше часу на те, заради чого ви прийшли – здійснення кампанії.

Успіхів!

Роббі Мук
Керівник виборчого штабу Гіларі Клінтон у 2016 р



Метт Роудс
Керівник виборчого штабу Мітта Ромні у 2012 р.

P.S. — У вас є ідея, як можна покращити цю стратегію? З'явились нові технології або слабкі ланки, які ми маємо взяти до уваги? Ми хочемо почути це від вас. Будь ласка, поділіться своїми ідеями, історіями та зауваженнями на Twitter @d3p, використовуючи хештег #CyberPlaybook, або надішліть нам електронний лист на адресу: connect@d3p.org, щоб ми могли продовжувати вдосконалювати цей ресурс по мірі змін у цифровому середовищі.

Автори та дописувачі

Цей проект став можливий завдяки десяткам людей, які люб'язно присвятили йому свій час. Особлива подяка **Деборі Планкетт** за керівництво проектом та **Гаррісону Монскі** за написання матеріалу. Ми також у боргу перед зазначеними нижче людьми, які витратили незчисленні години на перегляд чорнових варіантів та розробку власного внеску.

КЕРІВНИКИ ПРОЕКТУ «НА ЗАХИСТІ ЦИФРОВОЇ ДЕМОКРАТІЇ»

Ерік Розенбах (Eric Rosenbach), співдиректор Центру «Белфер»

Роббі Мук (Robby Mook), науковий співробітник Центру «Белфер»

Метт Роудз (Matt Rhoades), науковий співробітник Центру «Белфер»

АВТОРИ ТА ДОПИСУВАЧІ

Хізер Адкінс (Heather Adkins), директорка з безпеки інформації та приватних даних, Google

Дмітрій Альперович (Dmitri Alperovitch), співзасновник та технічний директор, CrowdStrike

Раян Боркенхаген (Ryan Borkenhagen), директор з інформаційних технологій, Комітет з проведення кампанії сенатора від Демократичної партії

Джош Бурек (Josh Burek), директор з глобальних комунікацій та стратегії, Центр «Белфер»

Майкл Чендерлін (Michael Chenderlin), головний спеціаліст з цифрових технологій, Definers Public Affairs

Роберт Коен (Robert Cohen), аналітик з питань кібернетичних загроз, K2 Intelligence

Кріс Коллінз (Chris Collins), співзасновник First Atlantic Capital

Кейтлін Конлі (Caitlin Conley), D3P, Harvard Kennedy School

Джулія Котрон (Julia Cotrone), асистентка з особливих питань, Definers Public Affairs

Джордан Д'Амато (Jordan D'Amato), D3P, Harvard Kennedy School

Мері Дугас (Mari Dugas), координаторка проекту, D3P, Harvard Kennedy School

Джош Фейнблум (Josh Feinblum), D3P, Массачусетський технологічний інститут

Джон Флінн (John Flynn), головний спеціаліст з інформаційної безпеки, Uber

Сіобхан Горман (Siobhan Gorman), директор, Brunswick Group

Деніел Гріггс (Daniel Griggs), засновник та генеральний директор, cmdSecurity Inc.

Стюартт Холлідей (Stuart Holliday), генеральний директор, Meridian International Center

Ебен Каплан (Eben Kaplan), головний консультант, CrowdStrike

Грег Кеснер (Greg Kesner), генеральний директор, GDK Consulting

Кент Лакен (Kent Lucken), управляючий директор, Citibank

Кетрін Манстед (Katherine Mansted), D3P, Harvard Kennedy School

Раян Макгіхан (Ryan McGeehan), член R10N Security

Джуд Мече (Jude Meche), технічний директор, Комітет з проведення кампанії сенатора від Демократичної партії

Нікко Меле (Nicco Mele), директор, Shorenstein Center

Ерік Мецгер (Eric Metzger), партнер-засновник та управляючий директор, cmdSecurity Inc.

Зак Моффатт (Zac Moffatt), генеральний директор, Targeted Victory

Гаррісон Монскі (Harrison Monsky), D3P, Harvard Law School

Дебора Планкетт (Debora Plunkett), колишня директорка з інформаційного забезпечення, Агентство національної безпеки

Колін Рід (Colin Reed), старший віце-президент, Definers Public Affairs

Джим Рут (Jim Routh), керівник служби безпеки, Aetna

Сюзанна Е. Спаулдінг (Suzanne E. Spaulding), старший радниця з питань внутрішньої безпеки, Центр стратегічних та міжнародних досліджень

Метью Спектор (Matthew Spector), D3P, Harvard Kennedy School

Ірен Солайман (Irene Solaiman), D3P, Harvard Kennedy School

Джефф Стамбольський (Jeff Stambolsky), аналітик з питань безпеки, CrowdStrike

Алекс Стамос (Alex Stamos), керівник служби безпеки, Facebook

Філ Венаблз (Phil Venables), партнер та Головний спеціаліст з оцінювання операційних ризиків, Goldman Sachs

Френк Вайт (Frank White), незалежний радник з комунікацій

Саллі Вайт (Sally White), D3P, Гарвардський університет

Роб Вітофф (Rob Witoff), старший менеджер з питань безпеки, Google

Дописувачі з **Національного демократичного інституту** та **Міжнародного Республіканського Інституту**

Від Міжнародного Республіканського Інституту, **Ян Суротчак**, **Стів ДіПанграціо**, **Керрі Шенкель** та **Кімбер Шеарер**.

Від Національного Демократичного Інституту, **Кріс Дотен**, **Еван Саммерс** та **Сара Моултон**.

Переклад на українську та російську мову став можливим завдяки **Джону Ловдалу**.

ГРУПА ВЕБ-РОЗРОБНИКІВ ТА ДИЗАЙНЕРІВ ЦЕНТРУ «БЕЛФЕР»

Аріель Дворкін (Arielle Dworkin), менеджер з цифрових комунікацій, центр «Белфер»

Ендрю Фасіні (Andrew Facini), координатор з питань друку та дизайну, центр «Белфер»

Підхід, що застосовується у Стратегії

Це європейське видання Стратегії D3P із забезпечення кібербезпеки під час кампанії було розроблено міжнародною командою експертів з питань кібербезпеки, політики та права, щоб запропонувати вам прості та дієві способи боротьби зі зростаючою кіберзагрозою.

Для кіберзлочинців немає різниці. Кампанії всіх рівнів, не лише широкомасштабні загальнонаціональні кампанії, ставали об'єктами їхніх атак. Ви повинні бути готові, що ви можете стати мішенню. Хоча рекомендації в цьому посібнику універсальні, вони, перш за все, призначені для кампаній, які не мають ресурсів для залучення професійного персоналу з кібербезпеки. Ми пропонуємо основні елементи кібербезпекової стратегії зменшення ризиків, яку можуть реалізувати люди без спеціальної технічної підготовки (хоча ми включили деякі речі, що потребують допомоги IT-спеціаліста).

Це – базові рекомендації, а не вичерпне керівництво з досягнення найвищого рівня безпеки. Ми заохочуємо всі кампанії залучати для надання професійної допомоги компетентних спеціалістів з інформаційних технологій та кібербезпеки, якщо це можливо.

Вступ

Кандидати та кампанії зіштовхуються з цілою низкою викликів. Потрібно організовувати заходи, набирати волонтерів, проводити демонстрації, залучати фінансування, контактувати з виборцями, реагувати на безжальні вимоги сучасного медіа-циклу. Кожен співробітник має враховувати можливість неприємних несподіванок, зокрема промахів або атаку критикуючими рекламними оголошеннями в останню хвилину. Кібератаки, кампанії з дезінформації та цензурування інтернету тепер також належать до цього переліку.

Оскільки кампанії стають все більшою мірою цифровими, зловмисники знайшли нові можливості втручатись, чинити перепони та красти. У 2008 році китайські хакери втрутились у кампанії Обами та МакКейна і вкрали у обох великі обсяги інформації. У 2016 році соціальні медіа були закриті під час виборів. У 2016 році кіберзловмисники, яких нібито фінансував російський уряд, вкрали та оприлюднили десятки тисяч електронних повідомлень і документів персоналу кампанії Демократичної партії США, сприяючи руйнівним кампаніям з дезінформації. У 2017 році політичні партії в Кенії зіштовхнулись

з масштабними дезінформаційними кампаніями, а сторінка Facebook ключової сербської політичної партії була виведена в оффлайновий режим.

Наслідки кібератаки можуть бути значними. Поширення інформації про сам злам, що супроводується поступовим оприлюдненням вкраденої інформації може місяцями негативно впливати на меседжі кандидата. Нападники, перевантажуючи веб-сайт, можуть перешкоджати комунікації з вашими прихильниками або зарахуванню внесків у найважливіщі моменти. Крадіжка персональних даних донорів чи виборців може призвести до значних юридичних наслідків, відкриває можливість переслідувати ваших прихильників чи викликати у донорів небажання робити внесок у вашу кампанію. Руйнівні напади на комп'ютери персоналу чи найважливіші сервери кампанії можуть уповільнювати темпи впровадження кампанії на дні або навіть тижні. Усунення безладу, який виник, може коштувати цінних ресурси у самий розпал перегонів, незалежно від того, чи це президентські або парламентські вибори, чи вибори до міської ради.

У найближчому майбутньому кіберзагрози залишаться реальною частиною виборчого процесу. Будучи на передовій лінії демократії, персонал кампанії повинен враховувати ризик атаки, розробити стратегію ефективного зменшення цього ризику і застосувати стратегії реагування тоді, коли трапилось найгірше. Хоча жодна кампанія не може мати гарантій повної безпеки, здійснення всього кількох простих кроків може значно ускладнити зловмисникам заподіяння шкоди. За іронією долі, найбільш досвідчені державні діячі часто обирають найпростіші методи нападу, атакуючи людей та організації, які нехтують базовими протоколами безпеки. Цей факт став основною причиною для розробки цієї європейської версії Стратегії забезпечення кібербезпеки під час кампанії.

У сьогоднішніх кампаніях кібербезпека – це відповідальність кожного. Людська помилка постійно стає першопричиною відомих кібератак, і завдання кандидата та керівників виборчих штабів полягає у тому, щоб включити обізнаність щодо безпеки у культуру партії. Рішення, які приймають люди, настільки ж важливі, як і програмне забезпечення, яке вони використовують. Продовжуючи цю думку, можна сказати, що найкращі кампанії повинні мати чіткі стандарти наполегливої роботи, донесення меседжу, відданості команді і крім цього – дотримання належного протоколу безпеки.

Перш, ніж ми перейдемо до рекомендацій, давайте швидко окреслимо проблему:

- **середовище**, у якому проходить ваша кампанія;
- **загрози**, які можуть постати перед вашою кампанією;
- **важливість** управління кібер-ризиками.

Вразливе середовище кампанії

Сьогоднішні кампанії – надзвичайно легкі мішені. Зазвичай за своєю природою вони тимчасові і швидкоплинні. На них немає часу та коштів розробляти довготермінові та добре перевірені стратегії безпеки. Буває, що велика кількість нового персоналу набирається без проведення тривалого навчання. Вони можуть приносити з дому власне обладнання – зі шкідливими програмами на ньому! Багато людей, які долучаються до кампаній, живуть та працюють за сотні кілометрів від штаб-квартири. Все швидко змінюється, ставки зазвичай високі, і людям здається, що у них немає часу перейматись кібербезпекою. Існує багато вірогідностей, що щось піде не так.

У той самий час, кампанії все більше покладаються на особисті дані виборців, донорів та на громадську думку. Вони також зберігають чутливу інформацію, таку як дослідження щодо опозиції, вразливі сторони, списки прихильників, дані спеціальної перевірки працівників, попередні версії політичних документів та електронні листи.

Ризики можливої атаки зростають, так само як і їх потенційні наслідки.

ЗАГРОЗА НАПАДУ

Уявіть: До дня виборів залишився місяць, і відрив між суперниками невеликий. Зранку ви прибуваєте до штаб-квартири, наливаєте собі кави або чаю, підходите до свого столу і включаєте комп'ютер. Ви бачите чорний екран, потім жахливу карикатуру на вашого кандидата, за якою з'являється повідомлення. Ваші жорсткі диски були відформатовані. Кожен цифровий біт інформації, яку ви збирали – документи, списки адрес, балансові звіти– все зникло. Ви читаєте – щоб повернути це все, вам треба

заплатити добрий мільйон, або ви втратите важливу політичну посаду.

Невідома група хакнула ваш комп'ютер кілька місяців тому і тихенько крала електронні листи, стратегічні документи, адреси донорів та номери полісів соціального захисту або ідентифікаційні номери ваших працівників. Ця група витратила тижні, пробираючись крізь величезні обсяги даних у пошуках брудної білизни, і поширювала новини про головні події кампанії у соціальних медіа та на легкому у використанні веб-сайті, присвяченому виключно поширенню такої інформації. На головній сторінці – матеріал про вашого кандидата з можливістю самостійного пошуку деталей, які цікавлять користувача. На даний момент веб-сайт кампанії «лежить», доступ до акаунтів в соціальних мережах тимчасово закрито через поширення непристойних фото, а працюючого комп'ютеру поблизу немає.

Загрози, які постають перед виборчою кампанією

На жаль для кампаній та демократій в усьому світі, місцеві та іноземні зловмисники можуть вважати, що завдання шкоди або допомога конкретному кандидату сприяє їм у досягненні їхніх інтересів, чи то сіяння хаосу і плутанини серед виборців, чи то покарання посадової особи, яка проти них виступила. Можливо, це звучить як якийсь трилер, але реальність така, що розвинута розвідка, кіберзлочинець або ображений на кандидата хакер-активіст можуть обрати вас або когось із вашої кампанії мішенню для себе. Це загрози, можливість яких мають усвідомлювати керівники та працівники кампанії.

Оскільки дезінформація і маніпуляції під час кампанії стає джерелом омани та обману громадян по всьому світу, викрадені дані, маніпулятивна подача інформації, витік інформації можуть мати реальні наслідки для ваших виборів. Механізми, встановлені для захисту ваших даних та забезпечення каналів комунікації тепер є важливими як ніколи.

ХТО ЗАЙМАЄТЬСЯ ХАКЕРСТВОМ?

Для виборчих кампаній багато хто може нести інформаційні та кібернетичні загрози. Поодинокі хакери та кіберзлочинці намагаються впливати на кампанії з причин особистої вигоди, прагнення слави або просто бажання перевірити, чи їм вдасться

це зробити. Національні держави становлять найбільш цілеспрямовану та постійну загрозу. Російські шпіонські групи, відомі як “Fancy Bear” (APT 28) та “Cozy Bear” (APT 29), підозрюють у хакерських нападах під час кампанії 2016 року у США. Китайські хакери значно більшою мірою зосередились на зборі інформації. Їх підозрюють у тому, що вони були активними під час президентських кампаній у США в 2008 та 2012 роках, але свідчення про оприлюднення ними вкрадених матеріалів відсутні. Хакери з Північної Кореї ганебно помстились Sony Pictures Entertainment за створення фільму «Інтерв’ю», викравши та оприлюднивши електронні листи та зламавши системи компанії. У деяких країнах загрозу для кампаній опозиції може становити уряд. Посилення міжнародної напруги, особливо навколо важливих виборів, може сприяти збільшенню кількості атак у майбутньому.

Управління кібернетичними ризиками

Ризик можна найкращим чином зрозуміти, взявши до уваги три фактори. По-перше, існують **вразливі місця** у вашій кампанії, які роблять інформацію вразливою до крадіжки, спотворення чи знищення. Вони можуть виникнути в апаратному чи програмному забезпеченні, на рівні процесів та внаслідок недостатньої пильності вашого персоналу. Також існують дійсні **загрози**: держави, хакери-активісти та інші недержавні групи, здатні використати ці вразливі місця. Ризик виникає там, де існують вразливі місця та загрози. І на останок, виникають **наслідки** – коли зловмисники заробляють гроші на ризиках, яких можна було уникнути.

Ви чи інші, хто залучений до кампанії мало що можете зробити, аби попередити самі загрози – вони є результатом ширших геополітичних, економічних та соціальних сил. Що ви *можете* зробити – це суттєво зменшити свою вразливість, тим самим знизити ймовірність того, що зловмисники досягнуть успіху. Зменшення вразливості знижує ризик, і вам вирішувати, які з вразливих місць найбільш важливі, щоб зменшувати там ризики. Наприклад, ви можете вирішити, що найбільшою шкодою, яку може заподіяти хакер, може бути викрадення звіту з результатами дослідження про кандидата, тому ви виділите додаткові ресурси для забезпечення зберігання у хмарному сховищі,

вимагатимете використання довгих паролів та надання доступу невеликій кількості осіб. Ви можете вирішити зробити інші документи кампанії більш доступними і менш захищеними, оскільки більше людей потребують їх для своєї роботи, і їхній витік не завдасть великої шкоди. Враховуйте, що заходи, які вживаються в рамках кампаній для збереження даних та реагування на кібернетичні зловживання, підпадають під дію законів щодо захисту даних та особистої інформації, які приймаються у всьому світі, наприклад Загальний регламент про захист даних (General Data Protection Regulation – GDPR) в Європейському Союзі.

Існують технічні аспекти для зменшення ризиків, і у нас є багато технічних рекомендацій, які ми включили у цей посібник, але найважливішим є цілісний підхід з вашого боку. Будучи керівником виборчої кампанії, найголовніше, що ви можете робити, це приймати основні рішення щодо того, хто матиме доступ до інформації, яка інформація буде зберігатись або відкидатись, скільки часу буде відводитись на навчання, а також якою буде ваша поведінка, щоб слугувати прикладом для інших. Оскільки ви є професіоналами, управління ризиками належить до сфери вашої відповідальності – технічної та людської. Ви визначаєте, які дані та системи мають найбільшу цінність, а також які ресурси ви будете виділяти на те, щоб їх захистити.

Забезпечення безпеки кампанії

Ми організували свої рекомендації щодо безпеки відповідно до трьох принципів:

1. Підготовка:

Успіх майже кожної рекомендації з цієї Стратегії залежить від створення керівництвом кампанії культури пильності щодо безпеки, яка мінімізує вразливі місця. Це означає встановлення основних правил, виконання яких забезпечується згори донизу, і які приймаються знизу догори.

2. Захист:

Захист відіграє вирішальну роль. Коли ви побачите, що маєте проблему з безпекою, то буде вже запізно. Побудова найсильнішого захисту, що його дозволяє час та ресурси, є ключовим для зменшення ризику. Безпека інтернету та даних працює найкращим чином на кількох рівнях – не існує єдиної «куленепробивної» технології чи продукту. Кілька основних заходів, що використовуються у поєднанні, можуть зробити цифрову архітектуру виборчої кампанії більш складною для зламу та більш стійкою, якщо її буде поставлено під загрозу, що загалом збереже час та гроші у майбутньому.

3. Наполегливість:

Сьогодні кампаніям загрожують суперники, рівень ресурсів та експертних знань яких постійно зростає; навіть найпильніша поведінка та найскладніша інфраструктура можуть не допомогти уникнути зламу систем безпеки. Кампанії мають планувати заздалегідь, що робити у разі зламу.

Деякі кампанії мають більше часу та грошей на забезпечення кібербезпеки, ніж інші. Саме тому наші рекомендації пропонують два рівні захисту: «**достатній**» та «**підвищений**». «Достатній» рівень відображає все, що кампанія має робити для того, аби мати мінімальний рівень безпеки. Ви завжди маєте прагнути робити більше, наскільки дозволяють час, гроші та людські ресурси, і тому ми рекомендуємо застосовувати «підвищений» рівень там, де це можливо. Якщо у вас є ресурси, щоб найняти авторитетних IT-спеціалістів, то це доцільно витрачені кошти. Загрози постійно розвиваються, тож професійні IT-послуги допоможуть вам досягнути більшого, ніж пропонується у нашому посібнику, а також дозволять вам бути в курсі останніх загроз і можливих рішень для вашої ситуації.

Керівництво

Керівники виборчої кампанії мають нести відповідальність за стратегію кібербезпеки, але більшість з них делегують розробку та нагляд своїм заступниками або керівнику служби оперативного управління. Важливо, щоб кібербезпека була щільно інтегрована до кадрової (HR) та інформаційно-технологічної (IT) роботи, оскільки правильне залучення працівників, апаратного забезпечення, а також контроль доступу будуть визначальними для вашої стратегії. Багато дрібних кампаній покладаються на підтримку волонтерів у сфері IT та кібербезпеки. Ви можете використовувати цей посібник у якості керівництва під час обговорення цих питань з волонтерами, які надаватимуть вам підтримку. Головне – це ретельно перевірити своїх волонтерів, які будуть на вас працювати, а також уважно контролювати доступ, щоб волонтерська підтримка не створювала нових вразливих ланок. Ви маєте переконатись, шо за IT-діяльністю наглядає працівник виборчої кампанії, якій також надає дозволи на доступ до різних систем.

Коли починати

Незалежно від того, яку модель підтримки ви маєте, **кібербезпека має починатись з першого дня**. Після цього має застосовуватись «Список перших п'яти пунктів», до яких входять найважливіші заходи. Переконайтесь, що вони були виконані з самого початку, навіть якщо у вас лише один або два працівники, а після цього забезпечте виконання решти рекомендацій «достатнього рівня» якомога швидше. Якщо ці заходи не були включені до вашого першого цифрового плану, не хвилюйтесь. Ще не запізно запровадити ефективні заходи безпеки та захистити те, що ви вже робите.

Вартість

Багато з того, що ми тут рекомендуємо, є безкоштовним або дуже дешевим. Власне, все, що входить до списку перших п'яти заходів, є безкоштовним, крім отримання платформи на базі хмарних технологій, що обійдеться вам лише в кілька доларів на місяць для кожного працівника. Широкомасштабні кампанії мають закладати в бюджет достатньо ресурсів на апаратне та програмне забезпечення, щоб реалізувати відповідальну стратегію, але це все одно має бути дуже невеликий відсоток багатомільйонного бюджету виборчої кампанії. Дрібніші кампанії зможуть реалізувати наведені тут рекомендації за суму від кількох сотень до кількох тисяч доларів залежно від того, скільки працівників або волонтерів будуть працювати в кампанії.

Будь-яке згадування постачальників або продуктів спрямоване на те, щоб допомогти навести приклади загальних рішень, але не означає, що ми рекомендуємо лише ці продукти. У разі виникнення проблем під час застосування продуктів або послуг, радимо вам звертатись до постачальників, які, як правило, можуть надати технічну допомогу на рівні користувача. Коли йдеться про вибір продукту чи послуги, заохочуємо порадитись з експертом з кібербезпеки або провести незалежне дослідження для того, щоб обрати найкращий продукт для своїх потреб.

Список перших п’яти пунктів

1. Створіть культуру обізнаності про інформаційну безпеку:

Сприймайте кібербезпеку серйозно. Візьміть на себе відповідальність за зменшення ризиків, навчайте своїх працівників та волонтерів і подавайте приклад. Людські помилки – найперша причина зламів.

2. Використовуйте хмарні технології:

Великий комерційний хмарний сервіс буде набагато безпечнішим, ніж будь-що з того, що ви можете запровадити з обмеженими ресурсами. Розгляньте можливість використання офісного пакету на основі хмарних технологій, наприклад, GSuite або Microsoft365, який забезпечить всі ваші основні офісні функції, а також створить безпечне місце для збереження вашої інформації (див. «Що таке «Хмара?» на с. 18).

3. Використовуйте двофакторну автентифікацію (2FA) та надійні паролі:

Вимагайте двофакторну автентифікацію (2FA) для того, щоб додати другий рівень захисту для всіх важливих акаунтів, включаючи свій офісний пакет, будь-які інші електронні скриньки чи сервіси збереження даних, а також власні облікові записи у соціальних мережах. Використовуйте мобільний додаток або фізичний ключ у якості свого другого фактору, а не текстове повідомлення. Для паролів створіть ЩОСЬДІЙСНОДОВГЕЯКЦЕЙРЯДОК, а не таке коротке, як Th1$. Всупереч загальнопоширеній думці, пароль, який складається з поєднання випадкових слів без символів, складніше зламати, ніж щось коротке з багатьма символами типу L0t$ 0f $ymB01$. Ніколи не повторюйте паролів; з цим вам також може допомогти менеджер паролів, який дозволить вам випадково генерувати потужні паролі та перевірить ваші поточні паролі, щоб визначити ті, які використовуються повторно.

4. Використовуйте зашифровані повідомлення для важливих розмов та матеріалів:

Використання шифрувального інструменту для телефонів, такого як Signal або Wickr, для важливих повідомлень та документів означає, що суперники не зможуть їх отримати, якщо «хакнуть» вашу поштову скриньку. Шифрування перемішує дані, що радикальним чином зменшує ймовірність того, що хтось зможе прочитати ваші повідомлення, навіть якщо вкраде дані.

5. Плануйте та готуйтесь:

Підготуйте план на випадок, якщо вашу систему безпеки буде зламано. Визначте, до кого звертатись за технічною допомогою, пам'ятайте про свої юридичні обов'язки та будьте готові до якомога швидшої та ефективнішої внутрішньої і зовнішньої комунікації.

Кроки із забезпечення безпеки вашої кампанії

Крок 1: Людський фактор

Кібербезпека – це головним чином людська проблема, а не технічна. Найкращі технічні рішення у світі не матимуть ефекту, якщо вони не будуть належним чином застосовуватися, або якщо вони не будуть постійно оновлюватись по мірі розвитку технологій. Успішні практики кібербезпеки залежать від створення безпекової культури.

"Достатній" — Що треба зробити

1. Створіть потужну культуру інформаційної безпеки, яка наголошує на тому, що безпека є стандартом для того, щоб виграти кампанію. Так само, як працівники виборчого штабу отримують вказівки не порушувати законодавство щодо фінансування кампанії, ці працівники повинні знати, що вони не мають натискати на посилання або відкривати додатки в електронних листах від невідомих відправників.

    a. **Залучення:** Організуйте базове навчання з інформаційної безпеки для нових працівників, яких ви залучаєте. Ви можете поширювати Роздатковий матеріал для працівників під час такого навчання (див. с. 15).

    b. **Навчання**: Зробіть безпеку частиною навчань, що проводяться для працівників, таких як заходи для працівників вищого рівня або тренінги із забезпечення явки виборців (GOTV) перед виборами. Організуйте додаткові навчання для тих, хто виконує важоиві ролі, тобто кандидата, працівників прес-служби, працівників вищого рівня, а також всіх, хто має права системного адміністратора у вашій мережі. Керівники повинні вимагати, щоб найважливіші люди в кампанії, включно із кандидатом, проходили перевірку налаштувань безпеки тими, хто відповідає за IT (це може бути сам керівник). Не соромтесь та не вагайтесь, коли йдеться про безпеку кандидата та інших важливих осіб!

    c. **Подавайте приклад**: Старші керівники кампанії та кандидат повинні виконувати помітну керівну роль, виступаючи за кібербезпеку під час тренінгів. Керівники вищого рівня мають періодично нагадувати про важливість кібербезпеки підлеглим під час зустрічей та телефонних розмов. Не обов'язково, тренінги мають проводити тільки експерти з технічних питань. Керівник виборчого штабу або начальник служби оперативного управління може донести більш потужний меседж саме тому, що підлеглі бачать його як менш «технічну» людину

2. Проводьте ретельну спеціальну перевірку працівників, волонтерів та стажерів – всіх, кому потрібний доступ до інформації кампанії, щоб уникнути надання реквізитів користувача комусь, хто хоче викрасти дані або підірвати роботу ваших систем.

    a. Розробіть визначення не публічної інформації та правила її використання. Наприклад, ви можете прийняти рішення засекретити інформацію про всі опитування, матеріали дослідження, стратегічні меморандуми та пов'язані з ними електронні листи як «чутливі».

    b. b. Забороніть передання приватної інформації через канали комунікації, які не управляються та не захищаються кампанією. Ви можете вимагати, щоб вона передавалась тільки у вигляді зашифрованих повідомлень (див. Крок 2).

3. Перевірте, щоб консультанти та постачальники, які мають доступ до приватної інформації, мали надійну електронну пошту та системи зберігання (див. Крок 2). У разі сумнівів вимагайте, щоб постачальники та консультанти використовували обліковий запис у вашому офісному пакеті в хмарній системі (див. Крок 2).

4. Контролюйте доступ до важливих онлайнових сервісів, таких як офіційні сторінки кампанії в соцмережах, щоб уникнути їхнього використання несанкціонованими особами. Переконайтесь, що ті, хто залишають кампанію, більше не матимуть доступу до її акаунтів. Це можна легко зробити за допомогою інструмента управління обліковим записом у соціальних мережах, який діє як "двері" до всіх ваших акаунтів. Якщо хтось залишає кампанію, ви маєте негайно відключити відповідний акаунт.

5. Проводьте навчання для працівників щодо загрози «фішингу». Переконайтесь, що вони знають, як розпізнавати та уникати підозрілих посилань, наголошуйте на важливості визначення та інформування про можливі фішингові атаки. У рамках частини потужної культури безпеки кампанії працівники вищого рівня повинні відзначати та заохочувати всіх, хто повідомляє про підозрілу поведінку у своїй системі, або визнає, що вони натиснули на потенційно шкідливе посилання.

6. Пам'ятайте про нормативно-правову базу. У деяких місцях, включаючи Європейський Союз, стандарти приватності передбачають певні обов'язкові вимоги щодо всієї інформації, яку може збирати ваша кампанія, особливо особисті дані, такі як демографічні дані чи адреси.

“Підвищений” — Зробіть наступний крок

1. Такі програмні продукти, як Phishme та KnowBe4, можуть навчати ваших працівників, надсилаючи їм фальшиві фішингові листи електронною поштою. Це безпечний, швидкий та ефективний спосіб дізнатись, стосовно кого є ризик, що вони натиснуть на посилання, тож ви можете провести для них додаткове навчання. Багато з таких продуктів також фільтрують деякі спроби фішингу у вашій електронній скриньці.

2. Якщо у вас є ресурси, найміть окремо IT-професіоналів, які будуть займатись системами вашої кампанії, та експерта з безпеки IT, який буде допомагати захищати, підтримувати та відстежувати цифрову структуру вашої кампанії. Цей експерт або експертка може проводити регулярне навчання з безпеки та перевіряти людей та системи, налаштовуючи безпекові рішення.

3. Укладіть договір з компанією, яка займається кібербезпекою і надасть безпекові рішення та перегляне захист та /або проведе моніторинг ваших систем на предмет зламу. Визначте, до якої кампанії ви будете звертатись, якщо вас «зламають» і вам знадобиться термінова підтримка та реагування. Це може бути альтернативою найму експерта з безпеки IT на повний робочий день. Проведіть аналіз ринку та оберіть компанію з гарною репутацією – не всі компанії у сфері кібербезпеки пропонують однаковий рівень послуг.

РОБОТА З ПРОФЕСІОНАЛАМИ У СФЕРІ БЕЗПЕКИ

Якщо ви приймаєте рішення працювати з професіоналом з безпеки, як ви оцінюватимете, чи це правильна людина або компанія? Незалежно від того, чи буде це особиста рекомендація або позитивні відгуки, важливо уникати фінансово дорогої, але неефективної підтримки. Під час інтерв’ю з потенційними експертами з питань безпеки, спитайте їх, як вони діяли в разі інциденту, пов’язаного з безпекою, і як вони створювали умови для більш безпечної роботи інших. Відповідний комітет вашої партії або працівники штабу, яким ви довіряєте, можуть порекомендувати кандидатів, з яких ви можете вибирати. Пам’ятайте, що культура впливає на безпеку, а також те, що навіть найкращі рекомендації можуть не допомогти досягти результату, якщо їх не виконувати (тобто просто укладення контракту з компанією в сфері кібербезпеки не вирішить ваших проблем).

Крок 2: Комунікація

Не всі методи комунікації є однаково безпечними, тож будьте свідомі щодо того, в який спосіб ви спілкуєтесь. Керівники кампанії повинні встановити стандарт, який заохочує особисті розмови завжди, коли це можливо, та не підтримує обмін непотрібними або зайвими електронними листами. Все, що ви пишете в електронному листі, може бути опубліковано в газеті або соцмережах – можливо, після зловмисної модифікації. Коли йдеться про телефонні дзвінки, текстові повідомлення або електронні листи – різні продукти та послуги пропонують різні рівні захисту, тож проведіть власне дослідження перш ніж обирати, які системи будуть використовуватись під час вашої кампанії.

"Достатній" — Що треба зробити

1. Для спілкування використовуйте якомога безпечніші системи.
    a. Використовуйте сервіси повного шифрування повідомлень, наприклад Signal або Wickr, особливо для надсилання повідомлень, поширення документів та здійснення телефонних дзвінків. Багато кампаній вимагають, щоб чутлива інформація передавалася лише у вигляді зашифрованих повідомлень, і часто для працівників кампанії найлегше звикнути використовувати ці додатки для всіх комунікацій (це особливо доречно для осіб з високим рівнем ризику, наприклад, кандидатів). Signal та Wickr публікують свій вихідний код для перегляду, та забезпечують функціональні характеристики, які зменшують ризик, наприклад, дозволяють вам автоматично видаляти повідомлення. Переконайтесь, що ваші повідомлення не синхронізуються з вашим комп'ютером або зашифрованими акаунтами у хмарах.
    b. Відключіть архівування сервісів текстових повідомлень, таких як Google Chat та Slack, щоб старі повідомлення з чатів не могли бути згодом викрадені. Для цього зайдіть в «налаштування» та виставте часові рамки «політики зберігання». Деякі сервіси вимагають цього для кожного окремого чату. Ми рекомендуємо зберігати повідомлення в чатах протягом одного тижня або навіть менше.
2. Використовуйте офісний пакет, розташований у хмарі, що забезпечує безпечне електронне листування, створення документів, розмови та обмін файлами, наприклад, GSuite або Microsoft365. Зокрема, GSuite включає Google Drive для обміну файлами, Gmail для електронного листування, Google Hangouts для розмов, а також Google Docs для обробки текстових даних, електронних таблиць та презентацій. Microsoft365 пропонує OneDrive/SharePoint для обміну файлами, Outlook/Exchange для електронного листування, Microsoft Teams для розмов та Microsoft Office для обробки текстових даних, електронних таблиць та презентацій. В разі якщо ви не наймаєте висококваліфікованих (та потенційно

дорогих) професіоналів з безпеки, то хмарні системи, які управляються провідними компаніями, надаватимуть більший захист, ніж будь-які сервери, які ви можете встановити у своєму виборчому штабі. Існують безкоштовні версії обох продуктів, але платні версії нададуть вам набагато більше можливостей адміністратора. Google також пропонує безкоштовні послуги для захисту організацій у загрозливому середовищі, такі як Outline, власний VPN; Project Shield – сервіс, що захищає ваш веб-сайт від спроб відключення; та Password Alert, який попереджає вас, якщо ви вводите свій пароль Gmail на фішинговому сайті.

ЩО ТАКЕ «ХМАРА»?

«Хмарні сервіси» забезпечують управління та доступ до інформації, що зберігається дистанційно в інтернеті. Вони підтримують оффлайнові сервери, якими управляють треті сторони; до них належать багато поширених сервісів які ви, можливо, вже використовуєте, наприклад Gmail або Dropbox. Добре, якщо ви зберігаєте інформацію за допомогою надійного провайдера сервісу хмарного сховища, а не на власному комп'ютері, оскільки такі провайдери мають кошти, технічні ресурси та експертні знання для того, щоб зробити свої послуги більш безпечними, ніж жорсткий диск на вашому лептопі або офісний сервер. Вони також мають достатньо технічного персоналу, який працює для захисту від складних атак на їхні мережі (тож і на ваші дані також). Це можна порівняти зі збереженням готівки під матрацом або у захищеному сейфі в банку. Використання хмарних сховищ пропонує додатковий запобіжник проти втрати даних, якщо персональний пристрій буде загублений або зламаний. Збереження у хмарі є опцією, що включається у комплексні послуги безпеки таких офісних пакетів, як GSuite та Microsoft365. До інших сервісів належить Dropbox або Box. Важливо пам'ятати, що до цих міжнародних корпорацій можуть застосовуватись законодавчі вимоги стосовно історії контактів, електронного листування або змісту файлів. Більшість провідних корпорацій, включаючи всі згадані тут, мають суворі політики щодо того, коли вони виконуватимуть ці вимоги.

3. Видаляйте електронне листування

    a. Включіть функцію автоматичного видалення у своєму додатку електронної пошти для старих електронних листів, щоб скоротити кількість листів, які потенційно можуть бути викрадені. Як правило, для цього вимагається зайти та змінити «Політику збереження» на більш короткий період у «Налаштуваннях». Щоб переконатись, що листи не залишаються у папці «Видалені», встановіть налаштування на автоматичне очищення

папки «Видалені» після закінчення певного проміжку часу. Ми рекомендуємо зберігати електронні листи протягом одного місяця або менше, якщо законом не вимагається зберігати їх довше. Те, чого ви не маєте, не можна викрасти.

4. Захищайте персональні облікові записи

    a. Справи кампанії ніколи не мають з'являтись в особистих акаунтах. Втім, опоненти будуть намагатись зламати особисті акаунти, тож забезпечте, щоб ваші працівники використовували надійні паролі та двофакторну верифікацію також для особистих облікових записів (це включено до Роздаткового матеріалу для працівників, див. с. 15).

А ЩО ЯК Я НЕ ДОВІРЯЮ ХМАРНОМУ СХОВИЩУ?

Деяким партіям не дуже подобається ідея довірити свою інформацію сторонній компанії. Якщо ви наполягаєте на тому, щоб мати власну технологічну інфраструктуру, пам'ятайте, що можливо вам доведеться захищати її від органів безпеки держав. Деякі міркування:

- На вас покладається відповідальність за розуміння, забезпечення безпеки та регулювання всіх аспектів у ваших системах, серверних додатках, програмному забезпеченні, базах даних та технологіях з'єднання.
- Вам варто переконатись, що зв'язок з вашими ключовими платформами є дуже надійним та не вразливим до маніпуляцій, цензури або DDOS.
- Вам потрібно буде активно відстежувати можливі злами та мати людину на зв'язку в режимі 24/7.
- Вам потрібно буде забезпечити безпечне дистанційне резервне копіювання.
- У разі існування ризику фізичного рейду всю вашу інформацію може бути вилучено.

ЩО ТАКЕ ШИФРУВАННЯ?

Шифрування – це спосіб кодування інформації під час її передачі між користувачами або збереження такий спосіб, щоб її міг прочитати лише визначений отримувач. Уявіть собі: користувач «переплутує» дані, коли їх надсилає, і тільки визначений отримувач має ключ, щоб все це розплутати. Буде доцільно використовувати шифрування, особливо для чутливої інформації, тому що навіть якщо зловмисник викраде дані, малоймовірно, що він зможе їх прочитати. Більшість додатків, що використовують шифрування, наприклад Signal або Wickr, роблять цей процес непомітним. Наскрізне шифрування є важливою складовою у комунікаційних програмах – це означає, що ваше повідомлення залишається секретним від вашого телефону або комп'ютера на всьому шляху до точки призначення, і ніхто – включаючи самого провайдера додатку – не може читати повідомлення. Якщо це можливо, також використовуйте шифрування всього диску на своєму лептопі; якщо його викрадуть або ви залишите його в автобусі, ніхто не зможе прочитати зміст.

ЦЕНЗУРА, СТЕЖЕННЯ ТА ВІДКЛЮЧЕННЯ ІНТЕРНЕТУ

На жаль, у багатьох куточках світу ширяться тенденції встановити контроль над відкритим демократичним простором інтернету. Ці тенденції включають в себе блокування важливих каналів комунікації, наприклад, таких як WhatsApp або Twitter; цензурування ваших публічних веб-сайтів; агресивне відстеження громадян, які відвідують ваші онлайн ресурси, чи того, що роблять ваші працівники онлайн. У найгірших випадках, кількість яких небезпечно зростає, країна може навіть закрити доступ до інтернету.

Завжди треба мати запасний план. Якщо ваша партія або кампанія особливо залежить від веб-сайту вашої кампанії, зробіть так, щоб на вашій сторінці у Facebook була найважливіша інформація на той випадок, якщо ваш сайт буде заблокований або цензурований. Якщо ключовим каналом комунікації є WhatsApp, будьте готові використовувати СМС або майте резервний телефонний список з усіма номерами. Якщо відстеження веб-трафіку або діяльності працівників вашої кампанії онлайн може створити проблеми, розгляньте можливості для використання обхідних інструментів або анонімізаторів, наприклад Tor Browser[1], Psiphon[2] чи Outline[3] do-it-yourself VPN. Майте під рукою список журналістів, з якими ви працюєте, і у випадку посилення цензури або відключення інтернету, допоможіть їм висвітлити цей сюжет.

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

ПІДТРИМКА ВАШОГО ВЕБ-САЙТУ ОНЛАЙН

Веб-сайт вашої кампанії, скоріш за все, є однією з найважливіших публічних комунікаційних платформ, а також найлегшим способом для громадян дізнатися про вас. Це робить вашу присутність онлайн особливо привабливою мішенню для зловмисних хакерів або недобросовісних опонентів. Розгляньте можливості для використання керованих хостингових платформ, таких як Wordpress.com, Wix, або Google Pages, на яких ви не несете відповідальності за виконання обов'язків адміністратора з безпеки веб-сайту. Якщо ви хочете мати власний веб-сайт, переконайтесь, що ви є експертом, або що ви можете найняти професіоналів, які будуть захищати його від хакерів.

Все частіше хакери використовують розподілені атаки на відмову в обслуговуванні (англ. DDOS), щоб вивести сайт офлайн під час критичних періодів через величезні обсяги фіктивних запитів.

Мережі розподілу змісту (Content Distribution Networks – CDNs) дають можливість тримати кешовану копію вашого сайту на потужних серверах в усьому світі, завдяки чому майже неможливо «зламати» їх усі. Cloudflare та Google's Project Shield - два продукти, які можуть допомогти захистити ваші публічні веб-сайти.

Крок 3: Доступ та управління акаунтом

Одним з найскладніших аспектів безпеки є недопуск (надання обмеженого доступу для) неавторизованих користувачів. Це означає недопущення зловмисників до ваших даних та ненадання працівникам вашої кампанії доступу до інформації, яка їм не потрібна. Хоча може здаватися, що деякі наведені нижче рекомендації незручні у використанні, але хакери можуть скористатися помилками тих, хто цінує зручність понад безпеку.

ЩО ТАКЕ ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ?

Двофакторна аутентифікація – це другий рівень безпеки, що вимагає від користувача надати додаткове підтвердження, крім пароля. Другий фактор є дуже важливим, оскільки якщо ваш пароль буде вкрадено, зловмисник все одно не зможе зайти у ваш акаунт. Вам відомий ваш пароль, а другий фактор ви отримуєте у вигляді коду, згенерованого додатком, це фізичний ключ або навіть щось біометричне, наприклад, відбиток пальця.

“Достатній” — Що треба зробити

1. Вимагайте двофакторну аутентифікацію (2FA) для всіх систем та додатків. Уникайте текстових повідомлень (СМС) для двофакторної аутентифікації, тому що нападники можуть легко клонувати номер телефону та отримати доступ до текстових повідомлень. Існують кілька додатків 2FA, які працюють так само, як текстові повідомлення, зокрема Google Authenticator, Microsoft Authenticator та Duo Mobile. Ви також можете використовувати фізичний ключ FIDO («швидка ідентифікація онлайн»), який вставляється у ваш USB драйвер, наприклад Yubikey або Feitian. Корисним довідником сервісів, які надають або не надають 2FA, є веб-сайт “TwoFactorAuth.org”.
2. Паролі.
    a. Вимагайте використання довгих паролів. Як ми вже зазначали раніше, створюйте довгі та надійні паролі. Можливості сучасних комп’ютерів дозволяють зламати семизначний пароль за мілісекунди. Пароль, що складається з 20 або навіть з 30 знаків вимагає від хакера набагато довшого часу на злам. Оберіть послідовність слів, яку ви легко можете запам’ятати.

b. Не повторюйте паролі! Використовуйте різні паролі для різних акаунтів, щоб хакер не зміг зламати кілька акаунтів, якщо буде викрадений один пароль.

c. Для захисту працівників та волонтерів кампанії від фішингових атак передавайте паролі особисто або через шифровані повідомлення, що знищуються через короткий проміжок часу. Вимагайте запиту зміни паролів для центральних акаунтів у такий самий спосіб або через відеочат, щоб переконатись, що це дійсно працівник або волонтер кампанії. Ніколи не передавайте паролі через електронну пошту та не зберігайте/роздавайте їх за допомогою служби підтримки.

3. Користуйтесь менеджером паролів, наприклад LastPass, 1Password або Dashlane, які допоможуть вам легко керувати великою кількістю довгих надійних паролів. Водночас переконайтесь, що ваша система управління має довгий та надійний пароль і двофакторну аутентифікацію. На сьогоднішній день ми не рекомендуємо вам користуватись менеджерами паролів, вбудованими у такі браузери як Chrome, Safari та Firefox, які найчастіше є менш безпечними ніж згадані окремі менеджери.

4. Створіть окремі акаунти для адміністраторів та користувачів і дуже суворо обмежте доступ до акаунтів адміністраторів. Адміністратори також повинні мати два окремі акаунти кампанії – один суто для виконання своїх функцій адміністратора і ще один у якості звичайного користувача для всіх інших напрямків роботи кампанії. Це зменшить ймовірність того, що зловмисник зможе зламати акаунт адміністратора, отримавши доступ до всієї мережі.

5. Проводьте періодичні перевірки тих, хто має доступ до різних пристроїв та мереж. Негайно блокуйте доступ для тих, хто залишає кампанію. Одразу ж міняйте паролі у разі виявлення підозрілої активності. Щоб це було можливим, переконайтесь, що ваші працівники не мають спільних облікових записів користувачів.

МЕНЕДЖЕРИ ПАРОЛІВ

Менеджери паролів – це засіб збереження, відновлення та генерування паролів. Деякі навіть пропонують можливість автозаповнення паролю на сторінках входу до облікового запису. Менеджер паролів вимагає власного паролю для входу, який є єдиним паролем, який вам треба запам’ятати. Звісно, існує ризик, що якщо хтось зламає ваш менеджер паролів (таке траплялось), то він отримає всі ваші паролі. Але цей ризик майже завжди набагато менший ніж переваги, отримані завдяки унікальним сильним паролям до всіх ваших акаунтів, і його можна значно зменшити за рахунок двофакторної аутентифікації входу до вашого менеджера паролів. Під час проведення кампаній менеджери паролів інколи є доцільними для акаунтів, що мають кількох користувачів, тому що адміністратор може безпечно надавати доступ до них.

“Підвищений” — Зробіть наступний крок

1. Створюйте профілі користувачів для різних груп працівників кампанії, які автоматично надають відповідний рівень доступу. Різні групи працівників – волонтери, стажери, співробітники на місцях, керівники виборчого штабу – потребують доступу до різних ресурсів. Створення заздалегідь визначених профілів полегшує створення умов, за яких люди отримують доступ лише до тієї інформації, яка їм потрібна для роботи.

ХТО ТАКІ АДМІНІСТРАТОРИ?

Говорячи «мовою IT», адміністратор або адмін може надавати користувачам доступ або контроль до систем або інформації. Наприклад, будучи адміном системи електронної пошти, ви можете створювати облікові записи, змінювати паролі та встановлювати вимоги щодо довжини пароля і двофакторної аутентифікації для всіх облікових записів. В таких офісних пакетах, як GSuite або Microsoft 365, ви можете створювати групи, наприклад «Місцева команда» або «Комунікаційна команда». Робота адміна є дійсно важливою. Якщо адміністратор все робить правильно, інформація буде доступною лише тим людям, яким вона потрібна, що є основним з точки зору безпеки. Це означає, що прийняття рішення про те, хто отримає права адміністратора, також має вирішальне значення. Лише кілька дійсно довірених та навчених осіб повинні мати можливість надавати іншим доступ до інформації. Якщо працівник із правами адміна залишає кампанію, переконайтесь, що такого працівника одразу ж було позбавлено відповідних прав!

Крок 4: Планування реагування на інциденти

Планування реагування у разі атаки є настільки ж важливо, як і розробка стратегії безпеки для її уникнення. Ваша реакція більше залежить від загальних наслідків інциденту ніж того, що було під загрозою. Ви маєте відвести певний час на обговорення з керівниками того, що станеться, якщо щось піде не так. Нижче наводиться контрольний список кроків, яких ви маєте вжити:

Правові

Визначте зовнішніх консультантів, яких ви запросите у випадку кібератаки, і обговоріть з ними процес реагування на початку кампанії. У більшості випадків це буде та сама людина, яка представляє вашу кампанію з інших питань, але в ідеалі це має бути хтось, хто спеціалізується на реагуванні на інциденти за викликом, безкоштовно або за суму, що сплачується за надання спеціальних послуг.

Попросіть свого юриста пояснити вам правові обов'язки у випадку викрадення даних, а також відповідні кроки, яких ви маєте вжити.

Пам'ятайте про правовий обов'язок ваших постачальників повідомляти вам або іншим у випадку, якщо вони стали об'єктами хакерської атаки. Якщо це можливо, включить суворі вимоги щодо попередження до угод з вашими постачальниками, оскільки треті сторони часто стають джерелом зламу.

Якщо ви вважаєте, що вас зламали, найкращою практикою буде дозволити вашому юристу стежити за реагуванням на умовах адвокатської таємниці.

Обговоріть зі своїм юристом найкращі шляхи співпраці з правоохоронними органами у випадку зламу. Кожна кампанія має свої підходи щодо цього.

Технічні

Визначте заздалегідь, до кого ви будете звертатись за технічною допомогою у разі хакерської атаки.

Оберіть особу в кампанії, яка буде підтримувати зв'язок з технічними експертами у разі зламу. В ідеалі це має бути та сама людина, яка відповідає за координування IT в кампанії. Робота з управління у випадку інциденту може бути величезною, тож вам буде потрібний хтось, хто зосередиться на технічних аспектах та знатиме, що треба робити. Це дозволить вам зосередитись на спілкуванні з зацікавленими сторонами та пресою.

З’ясуйте, яку технічну допомогу чи іншу підтримку вам можуть надати провайдери вашої платформи у разі кібернападу, наприклад, хакерської чи іншої атаки.

Операційні

Заздалегідь визначте, хто увійде до вашої команди з реагування на інциденти (IRT) та хто буде брати участь у засіданнях з реагування на інциденти. Важливо, щоб до цієї групи увійшов хтось з ваших команд IT, юридичних, операційних та комунікаційних команд. Якщо ви маєте маленький штаб та не маєте постійної комунікаційної, IT чи операційної підтримки, заплануйте включення до команди всіх ключових працівників кампанії, які керують її діяльністю.

Визначте ланцюжок підпорядкування для прийняття рішень у випадку зламу, особливо щодо комунікацій. У багатьох випадках це буде керівник виборчого штабу, але деякі керівники можуть вирішити делегувати відповідальність комусь іншому.

Визначте, який додаток або технологію ви будете використовувати для спілкування, якщо вважатимете, що ваші системи було зламано. Наприклад, якщо хакнуть вашу електронну пошту, ви можете покладатись на безпечний додаток для обміну повідомленнями, такий як Signal або Wickr. Комунікація під час зламу є вкрай важливою, але не треба, щоб опоненти знали, про що ви говорите – або навіть що ви реагуєте на їхні дії.

Комунікаційні

Сплануйте різні сценарії. Для багатьох кампаній це може бути частиною нарад щодо розробки стратегії. Для масштабніших кампаній з вищим рівнем ризику може бути необхідним проведення окремої наради.

Визначте ключових внутрішніх та зовнішніх гравців, наприклад, ваших працівників, волонтерів, донорів та прихильників. Пам’ятайте, кому треба повідомити у разі інциденту, та визначте порядок їхньої пріоритетності. Складіть список контактів та визначте, хто буде відповідати за зв'язок з ними.

Проведіть «мозковий штурм» щодо найгірших сценаріїв та визначте, як будуть змінюватись зацікавлені сторони та обмін повідомленнями у кожному з них. Потенційні сценарії можуть включати:

- Чутки про те, що вашу кампанію було зламано;
- Витік особистих даних ваших прихильників;
- Викрадення чутливої фінансової інформації донорів, такої як номера кредитних карток та контактів;

- Запуск вірусу-вимагача та спроб вимагання проти вашої кампанії;
- Стирання та закриття ваших систем;
- Викрадення електронного листування;
- Ваш опонент викрав облікові дані вашого адміністратора та всі файли з накопичувача вашої кампанії;
- Ваші акаунти в соціальних мережах було закрито або зламано;
- Відключено інтернет або окремі сайти, додатки або протоколи заблоковані в усій країні;
- Доступ до ключової інформації заблоковано або перервано через цензуру.

Обережно говоріть про свою політику кібербезпеки або про кібернапади. Деякі жертви кіберзлочинів у минулому робили грандіозні заяви про свої заходи безпеки або критикували тих, хто зазнав нападів. Преса покладе на вас відповідальність за те, що ви раніше казали, якщо ви самі стенете жертвою.

Так само не розголошуйте подробиць про обсяги на початкових етапах інциденту (якщо вам взагалі вдасться уникнути обговорення обсягів – навіть краще). Детальна інформація, наявна на початку, буде мінятись по мірі розслідування. Поширеною помилкою є заяви про те, що згодом виявляється неправдивим (наприклад, «Вони не дуже багато викрали» або «Жодних особистих даних не викрадено»). Найбезпечнішою тактикою буде говорити лише те, що вам точно відомо. Заяви мають зосереджуватися на діях, яких ви вживаєте, щоб виправити ситуацію для тих, на кого це вплинуло.

Заздалегідь підготуйте стандартні формулювання – в ідеалі після консультацій з вашими юрисконсультами, щоб можна було швидко написати заяву або тези для виступу у разі інциденту. Як мінімум, розробіть документ з типовими запитаннями та відповідями, який можна буде швидко переглянути, якщо вам доведеться його використовувати. Завчасна підготовка запитань та відповідей допоможе вам добре продумати те, чого ви не будете і що будете говорити. Наприклад, перше запитання найчастіше буде: «Що сталося?» Втім, може бути, що ви не зможете відповісти на нього протягом днів або тижнів. Те, що ви не знаєте, що саме відбудеться, власне може допомогти вам краще написати стандартні формулювання-відповіді заздалегідь.

ЗАПИТАННЯ ДЛЯ ВКЛЮЧЕННЯ ДО ВАШОГО ДОКУМЕНТУ ІЗ ЗАПИТАННЯМИ ТА ВІДПОВІДЯМИ:

- Що сталось?
- Як це сталось?
- Хто це зробив?
- Що було викрадено або пошкоджено?
- Чи було викрадено чиїсь особисті дані? Що ви робите для того, щоб їх захистити?
- Як хакери це зробили?
- Чи хакери більше не мають доступу до вашої системи?
- Як довго вони були у вашій системі?
- Які засоби безпеки ви застосовуєте? Чому вони не були ефективні?
- Чи не мали ви знати, що це станеться? Чому ваші системи не були краще захищені?
- Чи співпрацюєте ви із правоохоронними органами? Чи звертались до вас представники правоохоронних органів?
- У разі використання вірусу-вимагача вас спитають: чи заплатили ви суму, що вимагається? Чому ви заплатили або не заплатили?

Тримайте зв'язок зі своїми ключовими гравцями та надавайте їм всю можливу інформацію. Ймовірно, ви не зможете їм багато сказати, але регулярні контакти з ними, щоб повідомити, що саме ви знаєте, донести чітке повідомлення про свої наміри та дії для виправлення ситуації, відіграють ключову роль. Не дозволяйте, щоб від вас очікували занадто частого оновлення інформації, тому що часто у вас не буде нової інформації, і зацікавлені сторони почуватимуться розчарованими, якщо ви контактуватимете з ними, не надаючи нової інформації. Ініціюйте контактування зі ЗМІ тільки якщо ви можете повідомити їм щось нове.

Крок 5: Пристрої

Кожен фізичний пристрій у вашій кампанії – від мобільного телефона, планшета або ноутбука до роутера, принтера або фотоапарата – представляє собою потенційний шлях до вашої мережі. Гарний план кібербезпеки спрямований на забезпечення контролю доступу до та на всіх пристроях. Ви можете контролювати доступ до пристроїв шляхом забезпечення належного поводження з ними та ведення їхнього обліку. Ви контролюєте доступ до пристроїв за допомогою двофакторної автентифікації та надійних паролів. Ви контролюєте зміст, що зберігається на пристроях, за допомогою шифрування та політики збереження даних (тобто, збереження інформації у хмарних сховищах, не на комп'ютерах).

"Достатній" — Що треба зробити

1. Завжди використовуйте наявну найновішу операційну систему (ОС), оскільки системні оновлення регулярно включають патчи для останніх вразливих аспектів. Якщо це можливо, налаштуйте пристрій на автоматичне встановлення таких оновлень. Нехай до посадових обов'язків когось із працівників входить регулярна перевірка того, чи у всіх оновлені операційни системи.

2. Застосовуйте резервне копіювання! Для всіх даних, як ви зберігаєте на місцевому пристрої (наприклад, у своєму ПК), переконайтесь, що ви маєте план резервного копіювання на випадок фізичної крадіжки, поламки комп'ютера, або якщо ви проллєте каву на клавіатуру. Наприклад, ви можете використати сервіс резервного копіювання у хмарному сховищі для зменшення наслідків втрати даних. Приклади включають у себе Backblaze та CrashPlan.

3. Доступ до пристрою

    a. З самого початку керівництво кампанії має створити середовище, в якому люди серйозно сприймають фізичну безпеку своїх пристроїв – втрата пристрою може дати опоненту доступ до критичної інформації, що може зашкодити кампанії.

    b. Хоча багато кампаній не можуть дозволити собі придбання нових пристроїв, завжди, якщо є можливість, краще купити нове обладнання (особливо комп'ютери та телефони). Як мінімум, ви маєте забезпечити нові пристрої для працівників, які працюють з приватними даними або принаймні стерти чи переустановити операційні системи на відповідних старих пристроях. Якщо працівники використовують власні комп'ютери та телефони, запровадьте політику «Принеси власний пристрій» ("Bring

Your Own Device" (BYOD), що передбачає ретельний контроль безпеки (див. «Кінцевий захист» нижче).

c. Учасники кампанії НЕ повинні використовувати особисті акаунти електронної пошти або пристрої, які не були захищені відповідно до політики BYOD для діяльності у рамках кампанії, включаючи електронне листування та соціальні мережі. Вся важлива інформація, що знаходиться за межами пристроїв та систем, що контролюються кампанією, є вразливою до атак. Керівники повинні постійно наголошувати на тому, що дані кампанії мають залишатись поза особистими електронним скриньками та незахищеними комп'ютерами.

d. Підтримуйте фізичну безпеку своїх пристроїв. Перебуваючи у громадському транспорті, кафе або навіть у себе в офісі, завжди вживайте заходів для уникнення крадіжки пристроїв, що можуть надати доступ до ваших акаунтів, переписок та даних.

e. Повідомляйте про втрату пристрою негайно. Вимагайте, щоб налаштування за замовчуванням дозволяли дистанційно видаляти інформацію з усіх пристроїв. Приклади включають Find my iPhone та Android Device Manager.

f. Перемога чи поразка – майте готовий план, який передбачає, що робити з усіма даними, акаунтами та пристроями після завершення кампанії. Період одразу після кампанії є особливо вразливим.

4. Доступ до пристроїв

a. Змініть паролі та налаштування за умовчанням на всіх пристроях. Багато пристроїв доставляються від виробника з паролем за замовчуванням, який дуже легко вгадати. Крім цього, відключіть гостьовий акаунт, якщо він є на пристрої.

b. Встановіть автоматичне блокування на телефонах та комп'ютерах через дві хвилини та вимогу ввести пароль або надати відбиток пальця для розблокування.

c. Включіть автоматичне видалення для мобільних пристроїв, що передбачає видалення даних після певної кількості невдалих спроб входу.

5. Зміст на пристроях

a. Вимагайте шифрування на всіх пристроях (комп'ютерах та телефонах), щоб забезпечити, що втрата пристрою не означатиме витік його даних. Приклади включають у себе FileVault для Mac та BitLocker для Windows. Деякі пристрої, наприклад iPhone, роблять це за умовчанням, але не всі.

b. b. Встановіть програмне забезпечення для кінцевого захисту на всіх пристроях. Деякі приклади: Trend Micro, Sophos та Windows Defender. Існують спеціальні застосунки кінцевого захисту для телефонів і планшетів, наприклад Lookout.

ЩО ТАКЕ КІНЦЕВИЙ ЗАХИСТ?

Кінцеві точки – це пристрої, які використовують працівники, такі як мобільні телефони, ноутбуки та настільні комп'ютери. Вони є «кінцевими точками» мережі кампанії, а працівники є «кінцевими користувачами». Кінцевий захист централізовано контролює та управляє безпекою на дистанційних пристроях. Це особливо важливо для кампаній, які дозволяють працівникам використовувати власні пристрої (BYOD), оскільки кампанія має забезпечити безпеку пристрою, відсутність шкідливих програм на ньому, а також можливість стерти інформацію, якщо пристрій буде вкрадений або загублений. За допомогою кінцевого захисту також можна моніторити пристрій, щоб переконатись, що його програмне забезпечення оновлене, виявити шкідливі програми або потенційні загрози. Для багатьох кампаній це буде дуже обтяжливим, але включення цього до повсякденної роботи та відведення часу для цього заздалегідь вбереже вас від багатьох проблем у подальшому.

"Підвищений" — Зробіть наступний крок

1. Використовуйте програмне забезпечення з управління мобільними пристроями (mobile device management – MDM), яке відстежує діяльність, щоб переконатись, що всі пристрої відповідають політиці безпеки для мобільних телефонів та пристроїв користувачів, запровадженій у вашій кампанії. Приклади включають у себе VMware AirWatch, Microsoft InTune та JAMF. GSuite та Microsoft Office 365 також мають сервіс MDM.

2. Використовуйте розширені сервіси захисту від загроз, які відстежують та повідомляють про шкідливу активність, такі як CrowdStrike Falcon або Mandiant FireEye. Crowdstrike інколи пропонує сервіс попередження зламу Falcon безкоштовно через Crowdstrike Foundation в залежності від потреб вашої кампанії та правил фінансування кампанії.

Крок 6: Мережі

Мережі – це системи фізичного апаратного забезпечення, цифрове програмне забезпечення та зв'язки між ними. Вони представляють собою ще одне середовище, привабливе для атак. Безпека мережі включає у себе все – від того, як пристрої з'єднуються між собою, до використання хмарних сховищ для збереження даних.

"Достатній" — Що треба зробити

1. Зберігайте дані у перевірених хмарних сховищах, а не на персональних комп'ютерах або серверах. Все, що зберігається на персональному пристрої, має вищий ризик постраждати від зламу, крадіжки, нещасних випадків або рейдів ніж те, що зберігається у хмарі.
    a. Ніхто не повинен мати доступ до всіх файлів в мережі; акаунти з доступом адміністратора не повинні використовуватись у повсякденній роботі. Розділіть сховище ваших файлів на окремі папки та надавайте доступ тільки відповідним працівникам.
    b. Переконайтесь, що доступ до спільних файлів відкритий лише за запрошенням. Деякі сервіси управління файлами також передбачають визначення кінцевої дати, до якої дійсне запрошення та доступ.
    c. Регулярно перевіряйте, до чого і кому надається спільний доступ.
2. Майте окрему «гостьову» мережу wifi для відвідувачів та волонтерів, яка обмежує їхній доступ до ресурсів кампанії. Намагайтесь придбати роутери, які пропонують «гостьовий» профіль, що буде автоматично сегментувати вашу мережу. Ми дуже рекомендуємо вам змінити пароль мережі після завершення заходів кампанії, коли може мати місце велика плинність кадрів.
3. Під час подорожей або до створення штабу кампанії по максимуму уникайте використання публічного wifi та по можливості використовуйте надійні мережі wifi. Якщо вам потрібний мобільний wifi, спробуйте надати працівникам кампанії точки доступу мобільного wifi для прив'язки. Публічний wifi часто безкоштовний та легкий у під'єднанні, але зловмисники також можуть його використовувати для того, щоб проникнути до ваших комп'ютерів.
    a. Якщо це можливо, працівники мають використовувати VPN (віртуальна приватна мережа). VPNs допомагають захиститися від вторгнень під час використання публічного wifi. Приклади сервісів: ExpressVPN або TunnelBear. Не всі VPNs створені однаковими. Стережіться безкоштовних послуг: багато хто хоче зібрати ваші дані!

4. Захистіть свій браузер. PC Magazine визначив Chrome та Firefox як два найбезпечніших браузери у 2017 році. Незалежно від того, який браузер ви використовуєте, постійно його оновлюйте.

ЩО ТАКЕ VPN?

Віртуальна приватна мережа (VPN) – це зашифрований «тунель» для вашого інтернет-трафіку, який захищає його від вторгнень. Деякі офіси використовують його як засіб для дистанційного входу до офісної мережі, але це не дуже поширено під час кампаній. Виборчі штаби також мають розглянути можливість для використання їхніми працівникам VPN на комп'ютерах та мобільних телефонах, якщо їм часто доводиться використовувати громадський wifi або ненадійні мережі (що інколи доводиться робити працівникам під час подорожей або у місцевих осередках). Нещодавно Google випустив нову систему VPN під назвою Outline, яку можна самостійно встановити.

"Підвищений" — Зробіть наступний крок

1. Ви можете здійснити більш просунуті кроки для захисту власної мережі, але їх має виконувати IT-спеціаліст. Ми пропонуємо вам звернутися до спеціалістів з проханням забезпечити наступне:
    a. Встановити апаратний firewall (брандмауер, мережевий екран).
    b. Зашифрувати ваше wifi з'єднання за допомогою протоколів безпеки WPA2 або 802.1x (не використовуйте WEP).
    c. Конфігурувати веб-проксі на основі хмарних технологій для блокування доступу до підозрілих сайтів з будь-якого пристрою кампанії, незалежно від його місцезнаходження. Прикладами надавачів таких послуг є Zscaler, Cisco Umbrella та McAfee Web Gateway Cloud Service.
    d. Забезпечте збереження журналів активності у хмарному сховищі, наприклад LogEntries або SumoLogic.
    e. Сегментуйте те, що зберігається у хмарному сховищі, щоб не все зберігалось в одному місці. Дослідження щодо опозиції, стратегічні документи, файли працівників мають зберігатися у різних папках, а доступ до цих папок має надаватись тільки тим, кому потрібно надати такий доступ. Розгляньте можливість використання зовсім іншої системи збереження для найбільш важливої інформації кампанії. Обмежте доступ, щоб тільки головні працівники кампанії могли туди увійти і лише з визначених

пристроїв. (Наприклад, якщо ви використовуєте Microsoft365 для свого офісного пакету та збереження документів, зберігайте найбільш важливі документи в акаунті Dropbox або Box.) Якщо представник кампанії стане жертвою зламу, така сегментація дозволить зменшити нанесену шкоду.

2. Навчайте працівників не під'єднувати свої пристрої до невідомих портів або пристроїв. Не використовуйте громадські зарядки в аеропортах або на заходах. Не беріть безкоштовні телефонні зарядки або акумулятори на заходах (безкоштовний USB накопичувач може містити шкідливу програму!).

Крок 7: Інформаційні операції та зв'язки з громадськістю

Про інформаційні операції останнім часом багато говорилося в новинах, особливо про кампанії, що проводилися службами розвідки інших країн. Саме обрані лідери та політики приймуть рішення щодо того, як протистояти впровадження інформаційних операцій, і як працівники кампанії ми мало можемо вплинути, чи будуть вони впроваджені. Але ми можемо дещо зробити, щоб протистояти ним, якщо вони все-таки будуть запущені. Виборчі кампанії є та залишатимуться мішенню для таких операцій, і до цього треба готуватись. Захист того, як у рамках кампанії буде відбуватись спілкування з громадськістю, є важливою складовою процесу. Нижче наводяться кілька шляхів підвищення захисту від інформаційних операцій, визначення часу, коли вони плануються проти вашої кампанії або кандидата, а також оперативного реагування у разі, якщо це все-таки станеться.

ЩО ТАКЕ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ?

Інформація – це сила або принаймні так вважають численні військові та розвідувальні служби! Сила ідей вже довгий час живіть повстання та громадянські війни, і багато країн, які можуть мати слабші військові потужності у традиційному сенсі, намагаються використовувати інформацію, щоб розділити та відволікти своїх опонентів. Наприклад, в Росії вплив на громадську думку через пропаганду та провокацію місцевих конфліків

є частиною її доктрини ведення війни, яка постійно використовується проти тих, кого вважають опонентами. Соціальні медіа повністю змінили правила ведення інформаційних операцій. Зараз стало легше легко поширювати інформацію та видавати себе за інших, створюючи враження суспільного обурення або конфлікту..

"Достатній" — Що треба зробити

1. **Пам'ятайте: інформаційні операції – це комунікаційна проблема,** а не технічна. Суперники можуть підсилити свої інформаційні операції, викравши ваші дані, але коли інформацію буде оприлюднено, вам буде потрібна комунікаційна стратегія. Продумайте заздалегідь, що ви будете робити з фейковими або викривленими новинами – чи будете ви їх ігнорувати? Перепощувати та наголошувати, що це фейк? Як ви будете приймати відповідне рішення? Це одні з найбільш складних рішень, що їх доводиться приймати під час будь-якої кампанії, але найголовнішим є продумати ці питання у своїй команді заздалегідь, щоб ви та ваша команда мали уявлення, як реагувати, якщо ви взагалі будете реагувати.

2. **Знайте, що відбувається.** Заохочуйте активістів повідомляти про пости, сайти або новинні сюжети, які їм здаються підозрілими. Можете визначити певних стажерів або волонтерів, які будуть стежити саме за цим, проводити пошук для виявлення контенту, що публікується. Одним з постійних викликів є те, що неможливо слідкувати за всим, що з'являється у стрічці Facebook у ваших виборців. Ця платформа ускладнила публікацію політичної реклами та збільшила кількість працівників, які відстежують новинний контент, але ви не можете вивчати весь контент. Найкращим рішенням для цього на сьогоднішній день є визначення команди волонтерів, які представляють різні географічні та демографічні групи у вашому районі/окрузі, щоб ви змогли «виловити» якомога більше.

3. **Встановіть контакти з основними соціальними мережами та повідомляйте їм, якщо виявите фейкову або оманливу інформацію**. Більшість платформ соцмереж сьогодні видаляють фейковий або оманливий контент та профілі «самозванців». Зверніться до відповідного органу кампанії або до партії за відповідними контактами у соціальних медіа та встановіть зв'язок із ними на самому початку кампанії, щоб ви могли швидко звернутися до них, якщо щось піде не так.

    a. Facebook

    b. Twitter

    c. Google/Youtube

4. **Відстежуйте фейкові сайти**. Станом на сьогодні відсутні публічні повідомлення про самозванців, які намагаються красти гроші або дані про активістів через фейкові веб-сайти, але це є таким легким способом атаки, що варто бути обачливими. Переконайтесь, що ви придбали всі веб-адреси, які хочете використовувати (або які можуть бути використані проти вас). Можете найняти перевірену службу, яка буде здійснювати для вас моніторинг інтернету. Можна знайти людей, що робитимуть це за досить помірну ціну.

5. **Подбайте про захист проти атаки на відмову в обслуговуванні** (відома як DDoS). DDoS-атака відбувається, коли зловмисник бере під контроль велику кількість комп'ютерів та використовує їх одночасно, щоб «пінгувати» ваш веб-сайт, що виводить його з ладу. Більшість з того, про що ми говоримо у цьому посібнику, присвячена тому, як не допускати людей до даних вашої кампанії, але у випадку DDoS вам треба тримати свій веб-сайт відкритим та доступним весь час для донорів і активістів. DDoS-атаки поки що не стали загальнопоширеною загрозою для кампаній, але вони можуть використовуватись для того, щоб не дати вам збирати гроші або просто викликати збій у роботі вашої кампанії. Існує два безкоштовні інструменти, які ви можете використовувати для захисту свого сайту – Google Shield та Cloudflare.

Побачили, як можна покращити цю Стратегію?

З’явились нові технології або вразливі питання, які ми маємо вирішити?

Ми хочемо почути це від вас.

Будь ласка, поділіться своїми ідеями, історіями та зауваженнями на Twitter @d3p, використовуючи хештег #CyberPlaybook, або надішліть нам електронний лист на адресу: connect@d3p.org, щоб ми могли продовжувати вдосконалювати цей ресурс по мірі змін у цифровому середовищі.

Проект «На захисті цифрової демократії»
Центр «Белфер» з питань науки та міжнародних справ
Школа управління імені Джона Ф. Кеннеді
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P