BRUCE SCHNEIER

KLIKNIJ TUTAJ

ABY ZABIĆ WSZYSTKICH

BEZPIECZEŃSTWO I PRZETRWANIE
W HIPERPOŁĄCZONYM ŚWIECIE

Helion

Tytuł oryginału: Click Here to Kill Everybody:
Security and Survival in a Hyper-connected World

Tłumaczenie: Joanna Zatorska

Projekt okładki: Jan Paluch
Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock Images LLC.

ISBN: 978-83-283-5199-8

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/klitut
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

SPIS TREŚCI

WSTĘP: **WSZYSTKO STAJE SIĘ KOMPUTEREM** 9

CZĘŚĆ I: **TRENDY** 21

1. **NADAL TRUDNO ZABEZPIECZYĆ KOMPUTERY** 27
2. **POPRAWKI ZAWODZĄ JAKO PARADYGMAT ZABEZPIECZEŃ** 43
3. **CORAZ TRUDNIEJ SIĘ ZORIENTOWAĆ, KTO JEST KIM W INTERNECIE** 53
4. **WSZYSCY FAWORYZUJĄ BRAK BEZPIECZEŃSTWA** 65
5. **RYZYKA MAJĄ KATASTROFALNE SKUTKI** 87

CZĘŚĆ II: **ROZWIĄZANIA** 107

6. **JAK WYGLĄDA BEZPIECZNY INTERNET+** 115

7. **JAK MOŻNA ZABEZPIECZYĆ INTERNET+** 131

8. **RZĄD GWARANTEM BEZPIECZEŃSTWA** 155

9. **JAK RZĄDY MOGĄ NADAĆ WYŻSZY PRIORYTET DZIAŁANIOM OBRONNYM NIŻ OFENSYWIE** 171

10. **PLAN B. CO SIĘ PRAWDOPODOBNIE WYDARZY** 191

11. **CO MOŻE SIĘ NIE UDAĆ W POLITYCE** 203

12. **W STRONĘ ZAUFANEGO, ODPORNEGO I POKOJOWEGO INTERNETU+** 217

WNIOSKI: **POGODZENIE TECHNOLOGII Z POLITYKĄ** 225

PODZIĘKOWANIA 235

PRZYPISY 237

O AUTORZE 311

1

Nadal trudno zabezpieczyć komputery

Bezpieczeństwo jest zawsze kompromisem. Zwykle jest to kompromis między bezpieczeństwem a wygodą, ale czasem bezpieczeństwo konfrontuje się z funkcjonalnością lub wydajnością. Ponieważ zwykle nam na nich zależy, to one najczęściej odpowiadają za niedoskonałe zabezpieczenia komputerów. Należy jednak pamiętać, że bezpieczeństwo komputerów jest trudną sztuką.

W 1989 roku Gene Spafford, specjalista ds. bezpieczeństwa Internetu, wypowiedział te słynne słowa: „Jedynym prawdziwie bezpiecznym systemem[1] będzie ten, który pozbawimy zasilania, zatopimy w betonowym bloku i zamkniemy w ołowianym bunkrze pilnowanym przez uzbrojonych ochroniarzy. Jednak nawet w tym przypadku miałbym pewne wątpliwości". Niemal 30 lat później jego słowa nadal są aktualne.

Są one prawdziwe w przypadku niezależnych komputerów, a także tych podłączonych do Internetu komputerów wbudowanych we wszelkie urządzenia. Nieco później Rod Beckstrom, były dyrektor National Cybersecurity Center, podsumował to zjawisko w następujący sposób[2]: można się włamać do wszystkich urządzeń podłączonych do Internetu; wszystko podłączamy do Internetu; w efekcie wszystko jest narażone na atak.

Tak, komputery są tak trudne do zabezpieczenia, że każdy badacz bezpieczeństwa może się pochwalić trafnym podsumowaniem tego zjawiska. Oto mój wniosek z 2000 roku: „Bezpieczeństwo jest procesem, a nie produktem"[3].

Przyczyny są wielorakie.

OPROGRAMOWANIE JEST ZWYKLE KIEPSKO NAPISANE I NIEZABEZPIECZONE

Gram na swoim telefonie w grę Pokémon Go[4], która się ciągle zawiesza. Jest ekstremalnie niestabilna, jednak nie należy do wyjątków. Wszyscy znamy takie przypadki. Nasze komputery i smartfony regularnie się zawieszają. Witryny internetowe się nie wczytują. Funkcje nie działają. Nauczyliśmy się sobie z tym radzić. Kompulsywnie zapisujemy swoje dane i tworzymy kopie zapasowe plików lub korzystamy z systemów, które wykonują te zadania automatycznie. Restartujemy nasze komputery, gdy zaczynają się dziwnie zachowywać. Czasem tracimy ważne dane[5]. Nie oczekujemy też, że nasze komputery będą działać równie dobrze jak zwykłe produkty konsumpcyjne, chociaż ciągle frustrują nas wszelkie problemy.

Oprogramowanie jest słabo napisane, ponieważ — z nielicznymi wyjątkami — rynek nie promuje oprogramowania dobrej jakości. „Dobrze, szybko, tanio — wybierz dowolne dwie cechy"; niedrogie i szybkie wprowadzenie na rynek jest ważniejsze niż jakość. Dla większości z nas najczęściej słabo napisane oprogramowanie jest wystarczająco dobre.

Filozofia ta rozlała się na wszystkie poziomy w branży. Firmy nie promują jakości oprogramowania, a przecież promują dostarczanie produktów przed upływem terminów końcowych i z wykorzystaniem budżetu niższego niż zaplanowano. Uniwersytety skupiają się raczej na kodzie, który tylko działa, ignorując jego stabilność. Natomiast większość z nas — konsumentów nie ma ochoty na dopłacanie do lepszej jakości.

Nowoczesne oprogramowanie zawiera ogromną liczbę błędów. Niektóre z nich wynikają[6] ze złożoności oprogramowania — co rozwinę później — ale większość stanowią błędy programistyczne. Błędy te nie zostały naprawione podczas tworzenia programów; pozostają w oprogramowaniu po jego napisaniu i opublikowaniu. To, że takie oprogramowanie działa, zawdzięczamy naszym umiejętnościom korzystania z programów zawierających błędy.

Oczywiście nie wszystkie procesy tworzenia oprogramowania są identyczne. Po 2002 roku firma Microsoft poświęciła dekadę[7] na udoskonalenie procesu tworzenia oprogramowania, aby zminimalizować liczbę luk bezpieczeństwa w dostarczanych programach. Produkty tej firmy wcale nie są doskonałe — wykracza to poza możliwości współczesnej technologii — ale są znacznie lepsze niż średnia. Firma Apple słynie z oprogramowania wysokiej jakości[8], podobnie jak Google. Niektóre bardzo małe i krytyczne elementy oprogramowania są wysokiej jakości. Oprogramowanie sterujące elektroniką samolotów podlega znacznie bardziej rygorystycznym kryteriom jakości niż wszelkie inne. Natomiast NASA może pochwalić się słynnym procesem kontroli jakości[9], wykorzystywanym podczas tworzenia oprogramowania wahadłowców.

Przyczyny, dla których wspomniane przypadki należą do wyjątków, są różne w zależności od branży i przedsiębiorstwa. Firmy tworzące systemy operacyjne wydają duże kwoty; małe fragmenty kodu łatwiej napisać poprawnie; oprogramowanie samolotów podlega ścisłym przepisom. NASA nadal ma niezwykle konserwatywne[10] standardy zapewnienia jakości. A jednak nawet w systemach o dość wysokiej jakości, takich jak Windows, macOS, iOS i Android, nadal ciągle musimy instalować poprawki.

Niektóre błędy stanowią zagrożenie pod względem bezpieczeństwa. Niektóre mogą zostać wykorzystane przez agresorów. Przykładem może być[11] błąd wynikający z przepełnienia bufora. Jest to błąd programistyczny, który w niektórych przypadkach umożliwia atakującemu uruchomienie własnych poleceń i przejęcie kontroli nad komputerem. Podobne pomyłki mogą mieć przeróżną postać, przy czym niektóre z nich łatwiej popełnić niż inne.

Warto zauważyć, że trudno podać wartości liczbowe dotyczące wspomnianego zjawiska. Nie wiadomo, jaki odsetek[12] błędów stanowią błędy związane z bezpieczeństwem, a także jaki odsetek luk można wykorzystać do niecnych celów. W środowisku akademickim toczą się dyskusje, czy błędy możliwe do wykorzystania przez atakujących są stosunkowo rzadkie, czy może jest ich wiele. Osobiście skłaniam się ku temu drugiemu wariantowi. Wielkie systemy oprogramowania mają tysiące luk, które można wykorzystać, a włamanie się do tych systemów jest kwestią znalezienia jednej z nich — czasem jest to proste, a czasem nie.

Chociaż luk jest wiele, nie są one jednolicie rozlokowane. Niektóre z nich można z łatwością znaleźć, a inne są dobrze ukryte. Bezpieczeństwo oprogramowania można znacznie zwiększyć, stosując narzędzia, które automatycznie znajdują i naprawiają całe kategorie luk. To samo dotyczy praktyk programistycznych, które prowadzą do wyeliminowania wielu łatwych do znalezienia błędów. Jeśli ponadto ktoś znajdzie jakąś lukę, najprawdopodobniej ktoś inny niebawem też ją znajdzie lub już znalazł. Błąd typu heartbleed stanowi lukę w zabezpieczeniu sieci Web. Pozostawała ona nieodkryta przez dwa lata[13], gdy wreszcie dwóch badaczy wykryło ją niezależnie od siebie w przeciągu kilku dni. Luki o nazwie Spectre i Meltdown[14] występowały w podzespołach komputerowych przez co najmniej dziesięć lat, zanim kilku badaczy nie odkryło ich w 2017 roku. Nie potrafię znaleźć dobrego wytłumaczenia tych równoległych odkryć, po prostu tak się złożyło; jednak zjawisko to nabierze znaczenia, gdy w rozdziale 9. będziemy omawiać gromadzenie przez rządy luk w zabezpieczeniach, które można wykorzystać w celach szpiegowskich i jako cyberbroń.

Gwałtowny wzrost popularności urządzeń Internetu rzeczy (IoT) wiąże się z wykorzystaniem większej ilości oprogramowania, większej liczby wierszy kodu i jeszcze większej liczby błędów oraz zagrożeń. Aby utrzymać niskie ceny urządzeń IoT[15], zatrudnia się gorszych programistów, stosuje mniej rygorystyczne procesy tworzenia

oprogramowania i zwiększa ponowne wykorzystanie kodu. Wszystko to prowadzi do większych problemów, jeśli określona luka w zabezpieczeniach zostanie szeroko powielona.

Oprogramowanie, od którego jesteśmy zależni, czyli działające na naszych komputerach i telefonach, w samochodach i aparaturze medycznej, w Internecie i w systemach sterujących krytyczną infrastrukturą, jest wystawione na niebezpieczeństwo na wielu płaszczyznach. Nie jest to jedynie problem znalezienia kilku słabych punktów i ich naprawienia; jest ich po prostu za dużo. Musimy się pogodzić z tym, że w niedalekiej przyszłości będziemy musieli zmierzyć się z tym problemem.

INTERNETU NIGDY NIE PROJEKTOWANO Z MYŚLĄ O BEZPIECZEŃSTWIE

W kwietniu 2010 roku, przez około 18 minut[16] 15% całego ruchu internetowego nagle zostało przekierowane na trasy przechodzące przez serwery w Chinach. Nie wiadomo, czy to chiński rząd testował możliwości przechwytywania ruchu sieciowego, czy może była to zwykła pomyłka. Wiemy jednak, jak do tego doszło. Otóż atakujący wykorzystali zewnętrzny protokół trasowania, czyli Border Gateway Protocol.

Border Gateway Protocol, w skrócie BGP, opisuje fizyczne trasowanie ruchu w Internecie przez różne kable i inne połączenia między dostawcami usług, krajami i kontynentami. Ponieważ w systemie tym nie stosuje się uwierzytelniania[17] i każdy bezwarunkowo ufa wszystkim informacjom oraz szybkości i zagęszczeniu ruchu, protokół BGP można z łatwością zmanipulować. Na podstawie dokumentów ujawnionych[18] przez Edwarda Snowdena, byłego podwykonawcę rządowego, wiadomo, że agencja NSA wykorzystuje ten nieodłączny brak bezpieczeństwa, ułatwiając sobie przechwytywanie pewnych strumieni danych. W roku 2013 pewna firma donosiła[19] o 38 różnych przypadkach przekierowania ruchu internetowego przez routery dostawców usług w Białorusi lub Islandii. W 2014 roku rząd Turcji[20] wykorzystał tę technikę do ocenzurowania pewnych stron w Internecie. W 2017 ruch przychodzący i wychodzący[21] od niektórych amerykańskich dostawców usług został na krótko przekierowany przez routery nieokreślonego dostawcy Internetu w Rosji. Nie należy myśleć, że tego typu ataki ograniczają się do poziomu krajowego; na konferencji hakerów DefCon w roku 2008[22] pokazano, że każdy może to wykonać.

Gdy Internet był w fazie projektowania, kwestie bezpieczeństwa ograniczały się do fizycznych ataków na sieć. Opracowana wówczas architektura i dziś może sobie poradzić z awarią serwerów i połączeń. Nie może natomiast poradzić sobie z systemowymi atakami na wykorzystywane protokoły.

Podstawowe protokoły internetowe zostały opracowane bez uwzględnienia kwestii bezpieczeństwa. Wiele z nich do dziś nie doczekało się zabezpieczeń. Nie istnieje

zabezpieczenie odpowiadające polu „Od" w wiadomości e-mail. Każdy może udawać, że jest kimś innym. Nie ma zabezpieczeń w usłudze Domain Name Service, która tłumaczy adresy internetowe w postaci czytelnych przez ludzi nazw na adresy rozpoznawalne przez komputery, ani w protokole Network Time Protocol, który odpowiada za synchronizację wszystkich komponentów. Nie ma zabezpieczeń w oryginalnych protokołach HTML, które stanowią podstawę sieci World Wide Web. Nawet bezpieczniejszy protokół „https" nadal zawiera wiele luk. Wszystkie te protokoły są podatne na wykorzystanie przez agresorów.

Wspomniane protokoły zostały opracowane w latach 70. i na początku lat 80. XX wieku, gdy Internet był używany tylko w instytucjach badawczych i nie był wykorzystywany do żadnych krytycznych celów. David Clark, profesor w instytucie MIT oraz jeden z architektów wczesnego Internetu, wspomina: „Nie jest prawdą, że nie myśleliśmy o bezpieczeństwie[23]. Wiedzieliśmy, że niektórym ludziom nie można zaufać i wydawało się nam, że będziemy ich mogli wykluczyć". Tak, oni naprawdę myśleli, że zdołają ograniczyć użycie Internetu do swoich znajomych.

Jeszcze w roku 1996 panowało powszechne przekonanie, że za bezpieczeństwo będą odpowiadać punkty końcowe — czyli komputery obsługiwane przez ludzi — a nie sama sieć. Oto co w tymże roku stwierdzono w Internet Engineering Task Force (IETF), instytucji, która ustanawia branżowe standardy w Internecie:

> Jest wskazane, aby dostawcy Internetu[24] chronili prywatność i wiarygodność całego ruchu, jednak nie jest to wymagane na poziomie architektury. Za poufność i uwierzytelnianie odpowiadają użytkownicy końcowi. Cechy te muszą być zaimplementowane za pośrednictwem protokołów wykorzystywanych przez użytkowników końcowych. Punkty końcowe nie powinny być zależne od poufności ani integralności dostawców. Dostawcy mogą zapewnić pewien poziom zabezpieczeń, ale powinien on być jedynie uzupełnieniem podstawowego obowiązku użytkowników końcowych do ochrony samych siebie.

Powyższe stwierdzenia nie są takie głupie. W rozdziale 6. omawiam model sieciowy „od końca do końca" (*end-to-end*), w którym zakłada się, że sieć nie powinna być odpowiedzialna za bezpieczeństwo, zgodnie z zasadami opracowanymi przez IETF. Jednak ludzie za długo zbyt sztywno traktowali te zasady i nie udało się zapewnić nawet tych aspektów bezpieczeństwa, które mają sens jedynie jako integralny komponent sieci.

Poprawa tego stanu rzeczy okazała się trudna i niekiedy niemożliwa. Począwszy od lat 90. XX wieku, organizacja IETF zaproponowała dodanie zabezpieczeń do protokołu BGP w celu zapobiegania atakom, ale jej propozycje zawsze zderzały się z problemem zbiorczego działania. Wdrożenie bezpieczniejszego systemu przynosi

korzyści tylko wtedy, gdy obejmuje wystarczająco wiele sieci; ci, którzy dokonają wczesnego wdrożenia, odnoszą minimalne korzyści ze swoich starań. Prowadzi to do paradoksalnych sytuacji. Dostawca usług nie jest zainteresowany[25], aby jako pierwszy wdrożyć tę technologię, ponieważ będzie musiał ponieść koszty, chociaż nie uzyska żadnych korzyści. Warto poczekać, aż inni wykonają pierwszy krok. Oczywiście, wynik takiego podejścia możemy zaobserwować obecnie: 20 lat po zapoczątkowaniu dyskusji na temat tego problemu nadal nie udało się wypracować rozwiązania.

Podobnych przykładów możemy przytoczyć całe mnóstwo. DNSSEC jest aktualizacją, która mogłaby rozwiązać problemy z bezpieczeństwem protokołu Domain Name Service. Podobnie jak w przypadku BGP, istniejący protokół nie jest zabezpieczony i system może zostać zaatakowany na wiele różnych sposobów. Tak jak w przypadku BGP, upłynęło 20 lat[26], odkąd społeczność techniczna opracowała rozwiązanie, które jednak do tej pory nie zostało wdrożone. Wszyscy wiedzą, że korzyści pojawią się dopiero wtedy, gdy zostanie ono zaimplementowane przez większość serwisów.

ROZSZERZALNOŚĆ KOMPUTERÓW OZNACZA, ŻE WSZYSTKO MOŻE ZOSTAĆ UŻYTE PRZECIWKO NAM

Przypomnij sobie telefon, jakiego używali Twoi rodzice lub dziadkowie. Przedmiot ten został zaprojektowany i wyprodukowany jako telefon. Nie służył do niczego innego. Porównaj go z telefonem w swojej kieszeni. Właściwie nie jest to telefon, to komputer, na którym działa aplikacja telefoniczna. Jak wiesz, urządzenie to ma wiele innych funkcji. Można je wykorzystać jako telefon, aparat fotograficzny, system służący do wymiany wiadomości, czytnik książek, jako pomoc w nawigacji i do wielu innych celów. „Istnieje do tego aplikacja" nie ma żadnego sensu w odniesieniu do dawnego telefonu, ale jest oczywistością w przypadku komputera, który może wykonywać połączenia telefoniczne.

Po wynalezieniu prasy drukarskiej przez Johannesa Gutenberga około 1440 roku, technologia znacznie się poprawiła, ale przez kilka wieków opierała się na podobnym urządzeniu mechanicznym, a następnie elektromechanicznym. Przez ten czas prasa drukarska mogła jedynie drukować. Niezależnie od tego, jak bardzo starał się jej operator, nie można było za jej pomocą dokonywać obliczeń, odtwarzać muzyki ani zważyć ryby. Twój dawny termostat był urządzeniem elektromechanicznym, które mierzyło temperaturę i na jej podstawie włączało lub wyłączało dopływ prądu w przewodzie elektrycznym. Przewód ten był połączony z piecem, dzięki czemu termostat mógł włączać lub wyłączać ogrzewanie. To była jedyna funkcja, jaką mógł wykonywać. Natomiast dawny aparat fotograficzny mógł jedynie robić zdjęcia.

Współczesne wersje tych wszystkich urządzeń są komputerami, można zatem je zaprogramować, aby spełniały niemal dowolne funkcje. Niedawno hakerzy zaprezentowali te możliwości i tak zaprogramowali drukarkę Canon Pixma[27], termostat Honeywell Prestige[28] i aparat fotograficzny Kodak[29], że można było na nich zagrać w komputerową grę Doom.

Gdy opowiadam tę anegdotę na konferencjach technologicznych, wszyscy śmieją się na myśl o tych nowych urządzeniach IoT obsługujących 25-letnią grę komputerową, jednak nikt nie wydaje się zaskoczony. To są przecież komputery; wiadomo, że można je tak zaprogramować, aby na nich zagrać w grę Doom.

Inaczej reaguje na tę anegdotę publiczność mało obeznana z technologią. Zgodnie z naszym modelem myślowym, maszyny mogą wykonywać tylko jedną funkcję, a gdy się zepsują, przestają działać. Jednak komputery o ogólnym przeznaczeniu bardziej przypominają ludzi: mogą robić niemal wszystko.

Komputery są rozszerzalne. Ponieważ wszystkie rzeczy zaczynają nosić znamiona komputerów, rozszerzalność będzie dotyczyć wszystkiego. Ma to trojaki wpływ na bezpieczeństwo.

Po pierwsze, systemy rozszerzalne bardzo trudno zabezpieczyć, ponieważ ich projektanci nie są w stanie przewidzieć wszystkich konfiguracji, warunków, sposobów użycia itd. Wynika to ze złożoności, dlatego niebawem do tego wrócimy.

Po drugie, systemów rozszerzalnych nie można ograniczyć z zewnątrz. Łatwo zbudować mechaniczny odtwarzacz muzyczny, który odtwarza jedynie muzykę z taśm magnetycznych przechowywanych w określonym opakowaniu fizycznym. To samo dotyczy ekspresu do kawy, który wykorzystuje kapsułki określonego kształtu. Jednak te ograniczenia nie dotyczą świata cyfrowego. Oznacza to, że ochrona przed kopiowaniem — inaczej zarządzanie prawami cyfrowymi, czyli DRM (*digital rights management*) — jest właściwie niemożliwa. Zgodnie z doświadczeniami dotyczącymi branży muzycznej i filmowej z ostatnich dwóch dekad, nie jesteśmy w stanie zapobiec tworzeniu i odtwarzaniu nieautoryzowanych kopii plików cyfrowych.

Ogólnie rzecz biorąc, nie można ograniczyć systemu oprogramowania, ponieważ oprogramowanie ograniczające można zmodyfikować do innych celów, przepisać lub poprawić. Podobnie jak nie można utworzyć odtwarzacza muzycznego, który nie będzie odtwarzał nielegalnych plików muzycznych, tak samo nie można zbudować drukarki 3D, która odmówi drukowania części do pistoletu. Oczywiście, łatwo zabronić takich działań zwykłej osobie, jednak nie powstrzymamy eksperta. Gdy natomiast ekspert napisze już oprogramowanie, które obejdzie dowolne istniejące systemy sterujące, każdy z nas będzie mógł z niego skorzystać. Nie trzeba poświęcać na to wiele czasu. Nawet najlepsze systemy DRM[30] nie przetrwały 24 godzin. Wrócę do tego w rozdziale 11.

Po trzecie, rozszerzalność oznacza, że każdy komputer można uaktualnić za pomocą dodatkowych funkcji dostępnych poprzez oprogramowanie. W ten sposób można przypadkiem zainstalować luki bezpieczeństwa, które mogą się znajdować w kodzie nowych funkcji. Ponadto, nowe funkcje prawdopodobnie nie były przewidywane podczas wstępnego projektu. Jednak, co najważniejsze, nowe funkcje mogą zostać zainstalowane przez atakujących. Gdy ktoś włamuje się do komputera i instaluje złośliwe oprogramowanie, dodaje w ten sposób nowe funkcje. Są to funkcje, których nie potrzebujemy i nie chcemy, a które działają wbrew naszym interesom. Ponadto można je, przynajmniej w teorii, zainstalować na dowolnym istniejącym komputerze.

„Tylne drzwi" również są dodatkowymi funkcjami w systemie. W tej książce często używam tego terminu, dlatego warto się na chwilę zatrzymać i poznać jego znaczenie. Jest to dawny termin kryptograficzny[31], który ogólnie dotyczy dowolnego mechanizmu dostępu, celowo umieszczonego w systemie. Mechanizm ten umożliwia obejście zwykłych zabezpieczeń systemu komputerowego. Tylne drzwi zwykle pozostają tajemnicą — są umieszczane w systemach bez naszej wiedzy i zgody — jednak nie zawsze. Gdy FBI żąda[32] od firmy Apple obejścia szyfrowania iPhona, oznacza to, że agencja domaga się wprowadzenia tylnych drzwi. Gdy badacze znajdą w kodzie[33] dodatkowe hasło do zapór sieciowych Forinet, oznacza to, że znaleźli tylne drzwi. Gdy chińska firma Huawei umieszcza tajny mechanizm dostępu w swoich routerach internetowych, oznacza to, że instaluje w nich tylne drzwi. Zajmę się tym szerzej w rozdziale 11.

Wszystkie komputery można zainfekować złośliwym oprogramowaniem. Wszystkimi komputerami można sterować za pośrednictwem oprogramowania typu ransomware. Wszystkie komputery można przekształcić[34] w botnet, czyli w sieć urządzeń zainfekowanych złośliwym oprogramowaniem, którymi można sterować zdalnie. Wszystkie komputery można zdalnie wyczyścić. Nie ma znaczenia, jaką funkcję miał pełnić wbudowany komputer czy urządzenie IoT, które zawiera komputer. Atakujący mogą przejąć urządzenia IoT w każdy sposób, w jaki obecnie przejmują komputery stacjonarne i laptopy.

ZE WZGLĘDU NA ZŁOŻONOŚĆ SYSTEMÓW SKOMPUTERYZOWANYCH ŁATWIEJ PRZEPROWADZIĆ ATAK NIŻ SIĘ PRZED NIM OBRONIĆ

Współcześni agresorzy internetowi mają przewagę nad obrońcami.

Nie jest to nieuniknione. Przez dekady i wieki szala zwycięstwa przechylała się raz ku atakującym, a raz ku obrońcom. Studiując historię sztuki wojny, z łatwością zauważymy, że różne technologie, takie jak karabiny maszynowe i czołgi, dawały

przewagę raz jednej, a raz drugiej stronie. Jednak we współczesnym świecie zarówno w branży komputerowej, jak i w Internecie[35] atak jest łatwiejszy niż obrona. Wszystko wskazuje na to, że w przewidywalnej przyszłości sytuacja nie ulegnie zmianie.

Przyczyn takiego stanu rzeczy jest wiele, ale najważniejszą jest złożoność tych systemów. Złożoność jest największym wrogiem bezpieczeństwa[36]. Im bardziej skomplikowany system, tym mniej bezpieczny. A miliardy naszych komputerów[37], na których działa oprogramowanie złożone z dziesiątek milionów wierszy kodu, które połączone są do Internetu, w którym działają tryliony serwisów oraz przepływa nieznana liczba zetabajtów danych, tworzą najbardziej skomplikowaną maszynerię, jaką kiedykolwiek ludzkość zdołała zbudować.

Większa złożoność oznacza większą liczbę zaangażowanych ludzi, więcej części, więcej interakcji, więcej warstw abstrakcji, więcej błędów projektowych i w procesach programowania, większe trudności w testowaniu, więcej błędów w kodzie, w których mogą kryć się miejsca wrażliwe pod względem bezpieczeństwa.

Specjaliści ds. zabezpieczeń komputerów[38] lubią dyskutować o powierzchni ataku systemu, czyli o wszystkich możliwych miejscach, w które może celować atakujący i które należy zabezpieczyć. Złożony system cechuje się ogromną powierzchnią ataku, co stanowi ogromną korzyść dla potencjalnego agresora. Atakujący musi znaleźć tylko jeden słaby punkt — jedną niezabezpieczoną aleję, którą może poprowadzić atak — a następnie wybrać czas i metodę ataku. Może też prowadzić stały atak, aż uda mu się osiągnąć sukces. Jednocześnie obrońca musi zabezpieczać całą powierzchnię ataku, ciągle mając na uwadze wszystkie możliwe sposoby ataku. Podczas gdy obrońca musi zawsze wygrać, wystarczy, że atakujący będzie miał szczęście tylko jeden raz. Zasady tej bitwy nie są sprawiedliwe, a koszt ataku na system stanowi drobny ułamek kosztów, jakie należy ponieść na jego obronę.

Złożoność w dużym stopniu wyjaśnia, dlaczego nadal tak trudno zabezpieczyć komputery, mimo ciągłych ulepszeń technologicznych. Każdy rok przynosi nowe pomysły, nowe wyniki badań, nowe produkty i usługi. Jednocześnie rosnąca złożoność prowadzi do powstawania nowych luk i ataków. Tracimy grunt pod nogami, mimo że ciągle stajemy się lepsi.

Złożoność oznacza też, że użytkownicy często niewłaściwie pojmują bezpieczeństwo. Złożone systemy zwykle oferują wiele opcji, co utrudnia ich bezpieczne wykorzystywanie. Użytkownicy regularnie pomijają zmianę[39] domyślnych haseł lub niewłaściwie konfigurują kontrolę dostępu do danych w chmurze. W 2017 roku uniwersytet Stanforda[40] zrzucił winę na „niepoprawnie skonfigurowane uprawnienia", które doprowadziły do wycieku tysięcy rekordów danych dotyczących studentów i pracowników. Podobnych historii jest mnóstwo.

Atak jest łatwiejszy niż obrona nie tylko ze względu na złożoność. Atakujący mają przewagę pierwszego ruchu, a także naturalną zręczność, której zwykle brakuje obrońcom. Najczęściej nie muszą się przejmować kwestiami prawnymi, konwencjami moralnymi ani etyką. Ponadto mogą szybciej korzystać z innowacji technicznych. Ze względu na bieżący brak zachęt do poprawy, zupełnie nie radzimy sobie z proaktywnym zabezpieczaniem systemów. Dopóki nie dojdzie do ataku, rzadko podejmujemy prewencyjne działania związane z bezpieczeństwem. Atakujący mają też coś do zyskania, natomiast obrona zwykle wiąże się z dodatkowymi kosztami biznesowymi, które firmy chcą zminimalizować. Ponadto wielu zarządzających nadal nie wierzy, że ich firma może stać się celem ataków. Atakujący odnoszą coraz większe korzyści.

Nie oznacza to, że obrona jest daremna. Działania obronne są po prostu trudne i kosztowne. Oczywiście są łatwiejsze, jeśli atakujący jest samotnym przestępcą, którego można przekonać, aby zajął się łatwiejszym celem. Jednak wystarczająco uzdolnionemu, opłaconemu i zmotywowanemu agresorowi atak zawsze się powiedzie. O operacjach w cyberprzestrzeni na poziomie państwowym były wicedyrektor NSA Chris Inglis powiedział: „Gdybyśmy mieli przyznawać punkty w przestrzeni cyfrowej[41] w taki sam sposób jak oceniamy mecz piłki nożnej, wówczas po dwudziestu minutach gry wynik wynosiłby 462 – 456". Tak to właśnie wygląda.

Oczywiście, sam fakt, że ataki są łatwe pod względem technicznym, nie oznacza, że są rozpowszechnione. Morderstwo też można łatwo popełnić[42], ale niewielu się na to decyduje, ze względu na systemy społeczne służące do identyfikacji, piętnowania i karania morderców. W Internecie znacznie trudniej kogoś oskarżyć, ze względu na trudności w przypisaniu — czym zajmę się w rozdziale 3. Ponadto, międzynarodowy charakter ataków internetowych skutkuje trudnościami w prowadzeniu spraw sądowych.

Internet+ znacznie pogarsza sytuację. Więcej komputerów, a szczególnie więcej różnych rodzajów komputerów, oznacza większą złożoność.

WE WZAJEMNYCH POŁĄCZENIACH ZNAJDUJĄ SIĘ NOWE LUKI

Internet jest pełny nowych właściwości i niezamierzonych konsekwencji. Nawet specjaliści nie rozumieją zbyt dobrze, jak różne elementy Internetu na siebie oddziałują. Często dajemy się zaskoczyć, odkrywając, jak właściwie wszystko działa. Dotyczy to także luk w zabezpieczeniach.

Im ściślej łączymy ze sobą różne urządzenia, tym bardziej luki jednego systemu mają wpływ na inne systemy. Oto trzy przykłady.

- W 2013 roku przestępcy włamali się do sieci firmy Target Corporation i wykradli dane dotyczące 70 milionów klientów oraz 40 milionów kart kredytowych i debetowych. Przestępcy uzyskali dostęp43 do sieci firmy, gdyż udało się im ukraść dane dostępowe od jednego z dostawców systemu ogrzewania i klimatyzacji.
- W 2016 roku hakerzy przekształcili miliony komputerów IoT, takich jak routery, nagrywarki DVR, kamery internetowe itd. — w ogromny botnet o nazwie Mirai. Następnie za jego pomocą przeprowadzili rozproszony atak typu denial-of-service — tzw. atak DDoS — na dostawcę nazw domen Dyn. Firma Dyn dostarczała krytyczne funkcje internetowe dla wielu ważnych serwisów internetowych. Gdy urządzenia Dyn uległy awarii[44], wiele popularnych serwisów, takich jak Reddit, BBC, Yelp, PayPal i Etsy, przestało być dostępnych online.
- W 2017 roku hakerzy przeczesali[45] sieć nieznanego kasyna za pomocą połączonego z Internetem akwarium i ukradli dane.

Systemy mogą mieć wpływ na inne systemy w nieprzewidziany i potencjalnie szkodliwy sposób. To, co może się wydawać nieszkodliwe projektantom jakiegoś systemu, może przynieść szkody w połączeniu z innym systemem. Słabe punkty jednego systemu mogą w kaskadowy sposób przenieść się na inne systemy, co może doprowadzić do powstania zagrożeń, których nikt nie mógł przewidzieć. To w ten sposób mogło dojść do katastrofy atomowej na wyspie Three Mile Island, eksplozji wahadłowca *Challenger* lub przerwy w dostawie prądu w USA i Kanadzie w 2003 roku.

Omówione powyżej niezamierzone efekty prowadzą do dwóch konsekwencji. Po pierwsze, wzajemne połączenia utrudniają namierzenie systemu, który odpowiada za awarię. Po drugie, możliwe[46], że żaden z systemów nie jest w pełni odpowiedzialny za awarię. Przyczyną awarii może być niezabezpieczona interakcja dwóch bezpiecznych systemów. W roku 2012 ktoś przejął[47] konto Amazon reportera Mata Honana i w ten sposób uzyskał dostęp do jego konta w serwisie Apple, co z kolei umożliwiło mu uzyskanie dostępu do konta Gmail, a następnie do przejęcia kontroli nad kontem na Twitterze. Kolejność tych ataków ma znaczenie; niektóre z luk nie dotyczyły indywidualnych systemów, ale można je było wykorzystać tylko w połączeniu z innymi.

Można przytoczyć inne przykłady. Luki w zabezpieczeniach inteligentnych lodówek Samsunga[48] naraziły na atak konta Gmail użytkowników. Żyroskop w iPhonie[49], za pomocą którego wykrywa się ruch i orientację, jest wystarczająco wrażliwy, by wykrywać drgania akustyczne, co z kolei może doprowadzić do podsłuchiwania rozmów. Oprogramowanie antywirusowe firmy Kaspersky[50] przypadkowo (lub celowo) wykradało tajemnice rządu USA.

Jeśli 100 systemów komunikuje się ze sobą, mamy do czynienia z około 5000 interakcji i z taką samą liczbą potencjalnych luk, które mogą być wynikiem tych interakcji. Gdybyśmy rozważali 300 systemów, wówczas liczba interakcji wzrosłaby do 45 000. Tysiąc systemów oznacza pół miliona interakcji. Większość z nich jest nieszkodliwa, ale niektóre mają bardzo destrukcyjne konsekwencje.

KOMPUTERY ULEGAJĄ AWARIOM NA RÓŻNE SPOSOBY

Komputery nie psują się tak samo jak „normalne" rzeczy. Są wrażliwe na trzy różne i ważne sposoby.

Po pierwsze, odległość nie ma żadnego znaczenia. W rzeczywistym świecie zwracamy uwagę na zabezpieczenie się przed zwykłym agresorem. Nie kupujemy zamka do drzwi, który powstrzymałby najlepszych na świecie włamywaczy. Kupujemy taki zamek, który powstrzyma zwykłych włamywaczy. Takich, którzy mogą się włóczyć po naszej okolicy. Mam dom w Cambridge i nawet jeśli w Canberze grasuje niesłychanie uzdolniony włamywacz, nic mnie to nie obchodzi. Na pewno nie wsiądzie do samolotu i nie przeleci połowy świata, aby obrabować mój dom. Jednak w Internecie haker znajdujący się Canberze może z łatwością włamać się do mojej domowej sieci, podobnie jak do sieci domu po drugiej stronie ulicy.

Po drugie, możliwość atakowania komputerów można oddzielić od umiejętności ich atakowania. Oprogramowanie obejmuje umiejętności. Wyjątkowo utalentowany haker z Canberry może skorzystać ze swojej wiedzy o oprogramowaniu. Może zautomatyzować atak i przeprowadzić go nawet podczas snu. Może następnie przekazać swoje metody wszystkim zainteresowanym na całym świecie. Stąd wywodzi się termin „script kiddie", czyli skryptowy dzieciak, oznaczający osobę o niewielkich umiejętnościach, ale mającą dostęp do potężnego oprogramowania. Jeśli najlepszy na świecie włamywacz ma możliwość nieograniczonej dystrybucji narzędzia, które umożliwi zwykłemu włamywaczowi dostęp do Twojego domu, powinieneś poświęcić więcej uwagi jego bezpieczeństwu.

Wolna dystrybucja potencjalnie niebezpiecznych narzędzi hakerskich odbywa się w Internecie nieustannie. Agresor, który utworzył botnet Mirai[51], udostępnił swój kod światu, a w ciągu tygodnia kod ten został wbudowany do wielu narzędzi umożliwiających atak. Jest to przykład złośliwego oprogramowania: robaki, wirusy i rootkity, które dają ogromne możliwości nawet agresorom o niewielkich umiejętnościach. Hakerzy mogą kupić rootkity na czarnym rynku. Mogą wynająć ransomware w postaci usługi[52]. Firmy europejskie, takie jak HackingTeam[53] i Gamma Group, sprzedają narzędzia do przeprowadzania ataków mniejszym rządom na całym świecie. Russian Federal Security Service wykorzystało Karima Baratova, 21-letniego obywatela

Kanady pochodzenia kazachskiego, do przeprowadzenia ataku phishingowego, który doprowadził do skutecznego ataku na Democratic National Committee w 2016 roku. Złośliwe oprogramowanie zostało opracowane[54] przez utalentowanego hakera Alekseya Belana.

Po trzecie, komputery ulegają albo awarii całkowitej, albo żadnej. „Awaria klasy" to koncepcja dotycząca bezpieczeństwa komputerów[55]. Jest to szczególny rodzaj luki w zabezpieczeniach, która prowadzi do awarii nie tylko jednego systemu, ale całej klasy systemów. Przykładem może być luka w systemie operacyjnym, która umożliwia agresorom uzyskanie zdalnej kontroli nad wszystkimi komputerami, na których działa ten system operacyjny. Innym przykładem jest luka w cyfrowych nagrywarkach wideo oraz w kamerach internetowych, którą atakujący może wykorzystać do przekształcenia tych urządzeń w botnet.

W 2017 roku doszło do awarii klasy w systemie obsługującym dowody osobiste w Estonii. Wada kryptograficzna zmusiła rząd[56] do wycofania 760 000 dowodów wykorzystywanych w różnego rodzaju usługach rządowych, a niektóre były zabezpieczone wedle najwyższych standardów.

Zagrożenia wzrastają w wyniku istnienia monokultury oprogramowania i sprzętu. Prawie wszyscy z nas korzystają z jednego z trzech systemów operacyjnych i jednego z dwóch mobilnych systemów operacyjnych. Ponad połowa korzysta z przeglądarki internetowej Chrome; a pozostała połowa korzysta z jednej z pięciu innych. Większość z nas pisze teksty w programie Microsoft Word i korzysta z arkusza kalkulacyjnego Excel. Prawie każdy z nas czyta pliki PDF, ogląda pliki JPEG, słucha plików MP3 i odtwarza filmy z plików AVI. Niemal wszystkie urządzenia na świecie komunikują się za pośrednictwem tego samego protokołu internetowego TCP/IP. Ponadto, podstawowe standardy panujące w branży komputerowej nie są jedynym źródłem monokultur. Według badania z 2011 roku, przeprowadzonego przez DHS[57], GPS jest podstawą 11 z 15 krytycznych sektorów infrastruktury. Awarie klasy w tych i niezliczonych innych popularnych funkcjach i protokołach mogą z łatwością dotknąć miliony urządzeń i ludzi. Obecnie urządzenia IoT wykazują większe zróżnicowanie, ale sytuacja ta nie utrzyma się zbyt długo, chyba że zajdą zmiany w podstawowych zasadach gospodarczych. W przyszłości będzie się wykorzystywać jedynie kilka procesorów IoT, kilka systemów operacyjnych IoT, kilka sterowników i kilka protokołów komunikacyjnych.

Awarie klasy prowadzą do powstawania robaków, wirusów i innych złośliwych programów. Pomyśl o zasadzie „jednorazowy atak, wiele ofiar". Wydaje się nam, że oszustwo w głosowaniach polega na próbie głosowania przez nieuprawnione osoby, a nie na zdalnej manipulacji dokonywanej przez jedną osobę lub organizację na urządzeniach do głosowania podłączonych do Internetu czy też na listach

wyborców online. Jednak to właśnie tak wyglądają awarie systemów komputerowych: ktoś włamuje się do maszyn.

Wyobraźmy sobie kieszonkowca. Opanowanie niezbędnych umiejętności zajęło mu sporo czasu. Każda ofiara jest nowym zadaniem, a powodzenie w jednej kradzieży nie gwarantuje powodzenia w następnej. Elektroniczne zamki do drzwi, takie jakie obecnie stosuje się w pokojach hotelowych, mają różne słabe punkty. Atakujący może znaleźć lukę w projekcie, umożliwiającą mu utworzenie karty, za pomocą której będzie mógł otworzyć każde drzwi. Jeśli udostępni oprogramowanie służące do przeprowadzenia ataku, nie tylko on, ale wszyscy będą mogli otworzyć wszystkie zamki. A jeśli te zamki są podłączone do Internetu, atakujący może potencjalnie otworzyć je zdalnie — mógłby nawet jednocześnie zdalnie otworzyć wszystkie drzwi. To jest właśnie przykład awarii klasy.

Do podobnego ataku doszło w 2012 roku w firmie Onity[58], która produkuje zamki elektroniczne, zamontowane w ponad czterech milionach pokoi hotelowych, takich sieci jak Marriott, Hilton i InterContinental. Wykonane chałupniczo urządzenie umożliwiło hakerom otwarcie zamków w ciągu kilku sekund. Ktoś wymyślił sposób i instrukcje pozwalające na zbudowanie urządzenia szybko się rozpowszechniły. Firma Onity dopiero po kilku miesiącach[59] zorientowała się, że doszło do ataku hakerskiego, a ponieważ nie istniał sposób na załatanie luki (o czym opowiem w rozdziale 2.), pokoje hotelowe były narażone na atak przez wiele kolejnych miesięcy i lat.

Awarie klasy nie są nową koncepcją w zarządzaniu ryzykiem. Można je porównać do różnicy między włamaniami i pożarami domów, które zdarzają się czasem w różnych domach z sąsiedztwa w ciągu wielu lat, a między powodziami i trzęsieniami ziemi, które albo przytrafiają się wszystkim z sąsiedztwa, albo nikomu. Jednak komputery jednocześnie wykazują cechy tych wszystkich katastrof, a zarazem można się w nich doszukać pewnych aspektów modelu ryzyka związanego ze zdrowiem publicznym.

Ta natura awarii komputerowych zmienia naturę awarii zabezpieczeń i wywraca do góry nogami sposoby obrony. Nie przywiązujemy wagi do zagrożenia, jakie stanowi zwykły atakujący. Skupiamy się na najbardziej ekstremalnym przypadku, czyli osobie, która może zrujnować systemy wykorzystywane przez wszystkich.

ATAKI ZAWSZE SĄ LEPSZE, ŁATWIEJSZE I SZYBSZE

Standard szyfrowania Data Encryption Standard, czyli DES, jest algorytmem szyfrującym opracowanym w latach 70. XX wieku. Jego bezpieczeństwo zostało celowo zaprojektowane tak, aby był wystarczająco silny do odparcia ataków, które można było przeprowadzić w tamtych czasach. W 1976 roku specjaliści zajmujący się

kryptografią oszacowali[60], że zbudowanie maszyny zdolnej do złamania szyfru DES pochłonęłoby 20 milionów dolarów. W mojej książce z 1995 roku, zatytułowanej *Applied Cryptography*[61], oszacowałem, że koszt ten spadł do 1 miliona dolarów. W roku 1998 fundacja Electronic Frontier Foundation[62] zbudowała maszynę za 250 000 dolarów, która mogła złamać szyfr DES w czasie krótszym niż jeden dzień. Dziś możemy to wykonać na swoim laptopie.

W latach 90. XX wieku telefony komórkowe zaprojektowano w taki sposób, aby ufały wieżom przekaźnikowym bez żadnych systemów uwierzytelniania. Wynikało to z tego, że uwierzytelnianie było niełatwym zagadnieniem i trudno było zainstalować fałszywe wieże przekaźnikowe. Pół dekady później[63] urządzenia typu stingray, będące w zasadzie fałszywymi wieżami przekazującymi sygnał telefonii komórkowej, stały się tajnym narzędziem szpiegowskim wykorzystywanym przez FBI. Upłynęło kolejne pół dekady[64] i instalacja fałszywej wieży przekaźnikowej stała się tak łatwa, że hakerzy zaczęli prezentować swoje metody na scenach konferencji.

Także wzrastająca szybkość komputerów sprawiła, że zgadywanie haseł za pomocą ataku brute-force gwałtownie przyspieszyło. Metoda ta polega na wypróbowywaniu wszystkich kombinacji po kolei, aż do znalezienia poprawnej. Jednocześnie typowa długość i złożoność haseł, jakie zwykły człowiek jest skłonny zapamiętać, pozostała taka sama. W wyniku tego hasła[65], które były bezpieczne dziesięć lat temu, obecnie już takie nie są.

Następujący aforyzm usłyszałem po raz pierwszy z ust pracownika NSA: „Ataki zawsze są coraz lepsze; nigdy nie stają się gorsze". Ataki są coraz szybsze, tańsze i łatwiejsze. To, co dzisiaj pozostaje w sferze teoretycznej, jutro może znaleźć zastosowanie praktyczne. A ponieważ nasze systemy informatyczne istnieją dłużej niż planowaliśmy, musimy zacząć opracowywać plany z myślą o atakach na przyszłe rozwiązania technologiczne.

Atakujący też się uczą i dostosowują. To sprawia, że branża zabezpieczeń różni się od bezpieczeństwa. Tornada są kwestią bezpieczeństwa i można dyskutować o przeróżnych sposobach zabezpieczania się przed nimi oraz o ich różnej skuteczności, a także zastanawiać się nad tym, jak postęp technologiczny zapewni nam lepszą ochronę przed zniszczeniami. Jednak niezależnie od wybranych sposobów, wiemy, że tornada nigdy nie przystosują się do naszych metod obronnych i nie zmienią swojego zachowania. Są po prostu tornadami.

Przeciwnicy ludzcy zachowują się inaczej. Są kreatywni i inteligentni. Zmieniają taktyki, wymyślają nowe rzeczy i cały czas się przystosowują. Atakujący badają nasze systemy, szukając awarii klas. A gdy ktoś z nich jakąś znajdzie, będą z niej korzystać, dopóki luka nie zostanie załatana. Metody, które chronią obecnie sieci, mogą jutro zawieść, ponieważ atakujący mogą znaleźć sposób na ich obejście.

Wszystko to oznacza, że specjalistyczna wiedza szybko traci na znaczeniu. Wczorajsze ściśle tajne metody wojskowe dziś są tematami doktoratów, a jutro mogą stać się narzędziami hakerów. Przykładem może być kryptoanaliza różnicowa, wynaleziona przez NSA przed rokiem 1970. W latach 70. XX wieku wynaleźli ją także matematycy z firmy IBM[66] podczas opracowywania algorytmu DES. NSA utajniła odkrycie IBM[67], ale technikę tę ponownie wynaleźli kryptografowie akademiccy pod koniec lat 80. XX wieku.

Ochrona podlega ciągłym zmianom. To, co sprawdzało się wczoraj, dziś może się okazać bezużyteczne, a z pewnością nie będzie działać jutro.

Internet w coraz większym stopniu wpływa na decydujące kwestie naszej codzienności. Przez sieć komunikują się nie tylko komputery, ale i sprzęty gospodarstwa domowego, samochody, obiekty infrastruktury, takie jak elektrownie czy stacje uzdatniania wody, a nawet urządzenia do ratowania życia w szpitalach. Sterowanie nimi bardzo często odbywa się bez ciągłego nadzoru człowieka, a decyzje podejmują za niego algorytmy. To sytuacja bardzo wygodna dla użytkowników, ale też dla rosnącej rzeszy cyberprzestępców, którzy intensywnie korzystają z nowych możliwości. Kradzieże tożsamości, oszustwa, bezprawna inwigilacja, zaburzanie pracy systemów sterujących – na naszych oczach urzeczywistniają się coraz to bardziej przerażające scenariusze. Już dziś haker może dokonać morderstwa albo aktu terroru na wielką skalę.

Ta książka mówi o sprawach trudnych i niezwykle ważnych. Wszystkie komputery można zhakować, a kradzież danych to drobnostka w porównaniu z wrogim przejęciem jadącego samochodu, zakłóceniem pracy rozrusznika serca czy systemu kontroli krajowej sieci energetycznej. Poza konsekwencjami życia w świecie powszechnej sieci pokazano tu ukryte powiązania między technologią, polityką oraz gospodarką, przez które doświadczamy ogólnego braku bezpieczeństwa. Przedstawiono też – z myślą o firmach, rządach i osobach indywidualnych – sporo zdroworozsądkowych rozwiązań, dzięki którym można zminimalizować zagrożenia płynące z sieci. Bardzo ciekawie prezentuje się autorska wizja odporniejszego internetu rzeczy, podlegającego rozsądnym regulacjom i nadzorowi ze strony rządu. Książka jest lekturą obowiązkową dla każdego, kto chce zrozumieć prawidła rządzące tym zupełnie nowym środowiskiem i komu zależy na bezpiecznym rozkwicie ludzkości.

WYBRANE ZAGADNIENIA:

- NA CZYM POLEGAJĄ CYBERATAKI I JAKIE POWODUJĄ KONSEKWENCJE
- JAKIE SĄ SKUTKI INWIGILACJI I KONTROLI ORAZ ZYSKI Z BRAKU BEZPIECZEŃSTWA
- DLACZEGO BRAK BEZPIECZEŃSTWA JEST CHĘTNIEJ WYBIERANĄ OPCJĄ
- JAK ZABEZPIECZAĆ SWOJE URZĄDZENIA, POŁĄCZENIA I INFRASTRUKTURĘ
- CO MOGLIBY ZROBIĆ POLITYCY, ABY INTERNET BYŁ BEZPIECZNIEJSZY

BRUCE SCHNEIER – niekwestionowany światowy autorytet w dziedzinie bezpieczeństwa nowoczesnych technologii. Jest członkiem Berkman Klein Center for Internet and Society na Harvard University i wykładowcą nauk politycznych w Harvard Kennedy School, a także członkiem zarządu Electronic Frontier Foundation, Access Now oraz Tor Project. Pełni również funkcję specjalnego doradcy IBM Security i dyrektora technicznego IBM Resilient. Napisał kilkanaście książek oraz setki artykułów, esejów i publikacji naukowych. W Polsce ukazała się jego książka *Dane i Goliat. Ukryta bitwa o Twoje dane i kontrolę nad światem* (Helion, 2017).

LICZĄ SIĘ CZUJNOŚĆ I WIEDZA. CYBERWOJNA TRWA!

ISBN 978-83-283-5199-8
9 788328 351998
Cena: 39,90 zł