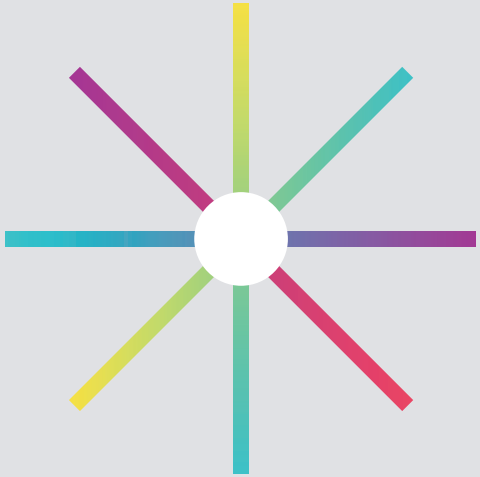
Poradnik w zakresie cyberbezpieczeństwa

na rok 2018:

Hakerzy i obrońcy cyberbezpieczeństwa wykorzystują zasady projektowania i uczenie się maszyn

Spis treści



Na całym świecie ludzie w coraz większym stopniu funkcjonują i pracują online, światy fizyczne i cyfrowe zaczynają się pokrywać, a waluty cyfrowe nie mające swego odpowiednika w realnym świecie, umożliwiają kupowanie rzeczywistych towarów i usług. Sztuczna inteligencja umożliwia autonomiczne podejmowanie decyzji przez pojazdy, codzienne znajdowanie potencjalnych nowych leków i personalizację zajęć lekcyjnych, aby pomóc uczniom w nauce.[1,2,3] Jednocześnie przy użyciu robotów lekarze przeprowadzają przez Internet ratujące życie operacje odbywające się na drugim końcu świata, a połączone z siecią czujniki zmieniają oblicze różnych branż — od wytwarzania energii po transport publiczny.[4] Z roku na rok lista branż korzystających z czujników, inteligentnych maszyn i mikroprocesorów wydłuża się.

Jedyna rzecz, która się nie zmienia, to fakt, że przy nadarzającej się okazji przestępcy i politycy o złych zamiarach wykorzystują luki w zabezpieczeniach dla własnego zysku. Wiele z narzędzi i technik, które przynoszą pokaźne korzyści społeczeństwu, ułatwia także przeprowadzanie złośliwych ataków i sprawia, że przynoszą one większe szkody. Złośliwe oprogramowanie, phishing i ataki typu „rozproszona odmowa usługi" (DDoS) to tylko niektóre z technik wykorzystujących w złych zamiarach przełomowe rozwiązania cyfrowe, dzięki którym świat idzie naprzód.

Dla specjalistów ds. bezpieczeństwa danych skuteczna obrona przed zalewem nieprzerwanych ataków przysparza nocnych koszmarów i zabiera spokojny sen. Kto wygrywa — hakerzy czy obrońcy?
Wobec faktu, że codziennie dochodzi do wielu skutecznych włamań, które zakłócają działalność firm i wywołują straty rzędu milionów dolarów w związku ze spadkiem wartości akcji, odpowiedź na to pytanie nie jest prosta.[5]

Aby przybliżyć czytelnikom aktualny i przyszły krajobraz cyberbezpieczeństwa, we współpracy z ekspertami z tej dziedziny opracowaliśmy niniejszy poradnik. Firma HP skorzystała z pomocy najbardziej doświadczonych specjalistów ds. bezpieczeństwa danych, aby pomóc decydentom odpowiedzialnym za zapewnienie bezpieczeństwa danych w firmach średniej wielkości i przedsiębiorstwach w zrozumieniu wszystkich dostępnych opcji zapobiegania szkodom związanym z brakiem odpowiednich zabezpieczeń.

Część 1:

Raport z sytuacji

Mniej więcej co cztery sekundy w Internecie pojawia się nowy egzemplarz złośliwego oprogramowania.

Obecnie na komputerach korzystających z oprogramowania antywirusowego tylko jednego typu odnotowuje się od 6 do 11 mln nowych infekcji złośliwym oprogramowaniem.[6] Około 700 ataków z użyciem techniki phishingu zostanie przeprowadzonych w nadziei skłonienia niczego nie podejrzewających osób do kliknięcia niebezpiecznego łącza, co pozwoli oszustowi wykraść ich dane osobowe lub uzyskać dostęp do sieci firmowej.[7] Mniej więcej co cztery sekundy w Internecie pojawia się nowy egzemplarz złośliwego oprogramowania.[8]

Nieznana liczba hakerów wydaje około 150 USD na wynajęcie botneta na tydzień w celu przeprowadzenia ataku typu „rozproszona odmowa usługi" (DDoS) mającego na celu zablokowanie serwisu online lub sieci przez wygenerowanie znacznego ruchu sieciowego[9]. Na całym świecie te ataki powodują łącznie wysyłanie do firm 500 Gb/s szkodliwych danych w celu zużycia przepustowości sieci i zablokowania obiektów docelowych.[10,11]

W międzyczasie miliony komputerów i połączonych z siecią drukarek, kamer, termostatów i innych urządzeń Internetu rzeczy (IoT) pozostają niezabezpieczone, bez zainstalowania najnowszych poprawek zabezpieczeń, a tylko kwestią czasu jest, zanim osoba o złych zamiarach znajdzie otwarte drzwi do najbardziej wrażliwych danych organizacji.[12]

Efektem jest stały napływ doniesień prasowych o skutecznych włamaniach do sieci, które powinny być bezpieczne. Już w pierwszych dniach roku 2018 oprogramowanie typu ransomware zablokowało sieć regionalnego szpitala, z żądaniem wniesienia opłaty w walucie bitcoin, a także zaatakowane zostały systemy komputerowe pewnego samorządu lokalnego i wszystkie systemy komputerowe szkoły w pewnym amerykańskim hrabstwie.[13,14,15] Równocześnie znaleziono poważną lukę w zabezpieczeniach mikroukładów, co mogło oznaczać, że każdy nowoczesny komputer bez zainstalowanej poprawki może być celem ataku.[16]

Oczywistym jest, że ataki te — niemal w całości przeprowadzane z pobudek finansowych — biorą na cel nie tylko takie grupy, jak banki indyjskie (2016 rok) czy duże organizacje, jak Sony, Equifax i Yahoo.[16] Hakerzy atakują także firmy małe i średniej wielkości, placówki służby zdrowia, urzędy miejskie i inne sieci.[18]
Bodziec finansowy jest tak duży, że zagrożenia mnożą się jak grzyby po deszczu. Jedna z przeprowadzonych analiz wykazała, że koszty związane z cyberprzestępczością do roku 2021 wyniosą 6 bilionów USD — tak, bilionów — więcej niż zyski ze światowego handlu narkotykami.[19]

Nie lekceważ tego, co oczywiste

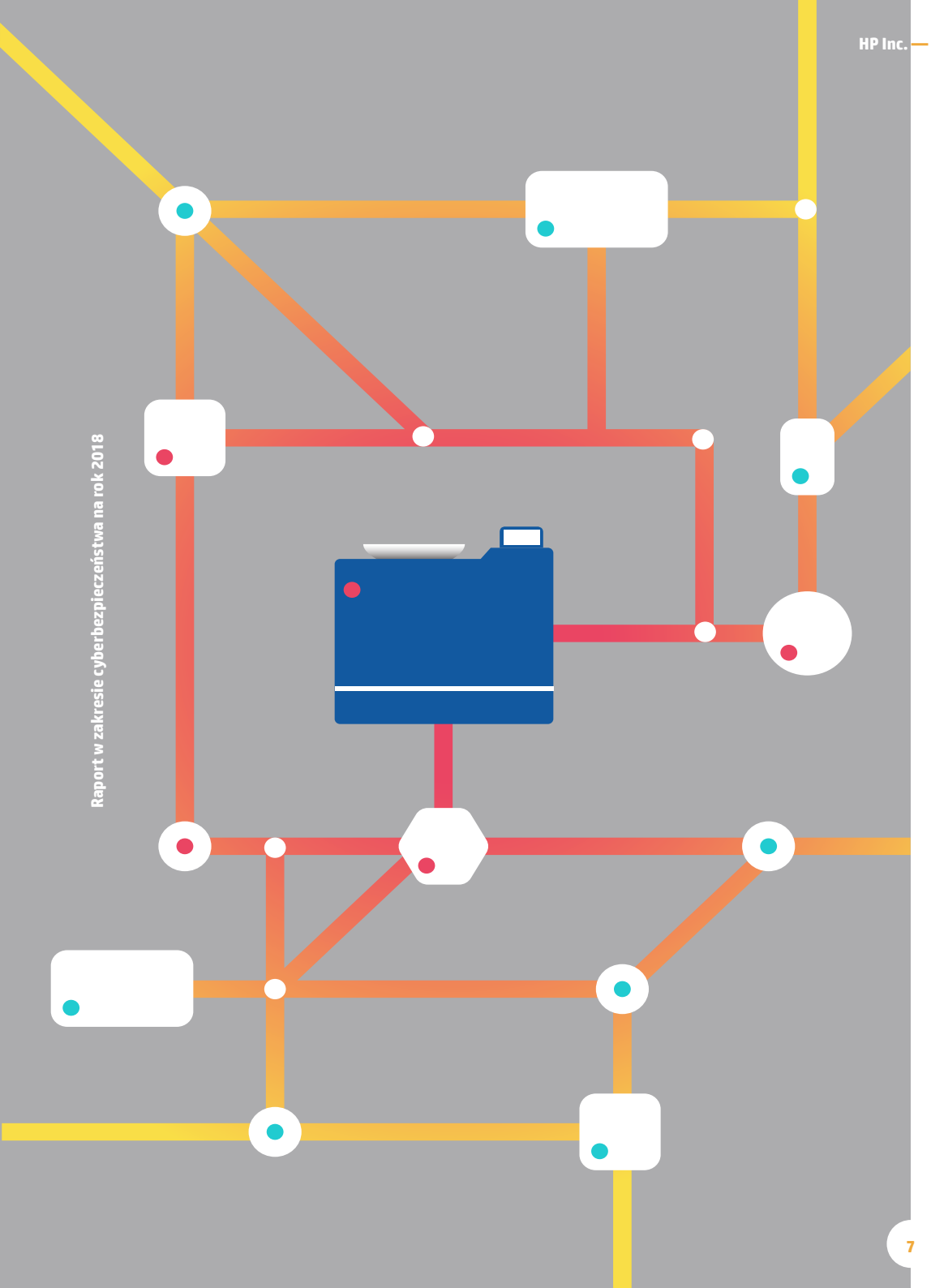
Wszystkie te zagrożenia są dobrze znane ekspertowi ds. bezpieczeństwa danych Jasonowi O'Keeffe, doradcy firmy HP ds. bezpieczeństwa druku. W jego opinii przestępcom bardzo pomagają nierozważne zachowania użytkowników komputerów oraz niewystarczające zabezpieczenia, co jest spowodowane brakiem lub niedostateczną liczebnością personelu zajmującego się cyberbezpieczeństwem.[20]

Analizując luki w zabezpieczeniach sieci komputerowych firm, O'Keeffe stwierdził występowanie szeregu problemów, które ułatwiają pracę hakerom, w tym poważnych niedopatrzeń działów IT, które powinny mieć większą orientację w tym zagadnieniu.

W trakcie analizy poproszono Jasona O'Keeffe o przyjrzenie się infrastrukturze IT dużego producenta. Pośród wielu innych problemów ekspert stwierdził, że hasła fabryczne nie zostały zmienione w 90% z 36 000 firmowych drukarek rozproszonych po całej sieci, co umożliwiało do nich dostęp każdej osobie, która wiedziała, w jaki sposób obejść poszczególne zabezpieczenia urządzeń. Dalsza analiza przeprowadzona przez Jasona O'Keeffe wykazała, że wiele drukarek było nieprawidłowo skonfigurowanych, co mogło pozwolić osobie postronnej na uzyskanie dostępu do drukarek i zmianę ich konfiguracji w celu wykradzenia danych z sieci lub ich przejęcia do pracy jako botnet. Jak wspomina O'Keeffe, „wiceprezes uderzył pięścią w stół i powiedział: <<Jason, czy Ty żarty sobie stroisz?>>". „Ten człowiek wrzał ze złości".

Wobec szybkiego rozpowszechniania się urządzeń IoT i innych urządzeń podłączonych do Internetu oraz do wewnętrznej sieci firmy, która nie wymaga właściwego uwierzytelniania, przestępcy mają do dyspozycji szybko powiększającą się liczbę punktów dostępu. Do przeszłości należą dni, gdy menedżer ds. bezpieczeństwa danych uważał pracę za skończoną po odpowiednim zabezpieczeniu serwerów o krytycznym znaczeniu dla działalności firmy. Obecnie zabezpieczenia muszą obejmować czasem miliony urządzeń połączonych z siecią w odległych oddziałach — i w kieszeniach pracowników.

„Staramy się zabezpieczyć komputery, serwery i inne kluczowe elementy sieci, ale to urządzenia IoT stwarzają obecnie dla sieci większe ryzyko" — powiedziała Shivaun Albright, główny technolog firmy HP ds. zabezpieczeń drukarek.[21] „Typowo na każde 100 wierszy napisanego kodu źródłowego występuje jeden defekt. Wystarczy zatem, że haker znajdzie defekt, który daje mu dostęp do systemu. Staramy się maksymalnie ograniczyć liczbę takich punktów ekspozycji na zagrożenia".



Dostęp w każdym miejscu

Ogromny potencjalny zysk rozbudza w dzisiejszych hakerach innowacyjność i kreatywność. Według Shivaun Albright do największych zagrożeń należą botnety — zautomatyzowane narzędzia złożone z tysięcy zhakowanych urządzeń IoT. Aby stworzyć botnet, oszuści przejmują procesory niezabezpieczonych urządzeń, a następnie wykorzystują zmanipulowane urządzenia do pozyskiwania środków w walucie bitcoin — ewentualnie wynajmują swoje botnety innym osobom do przeprowadzania ataków typu DDoS w celu uzyskania okupu.[22]

Wobec liczby stale przeprowadzanych prób włamań i wzrastającej liczby sposobów uzyskiwania dostępu przez hakerów, Jason O'Keeffe i inni eksperci twierdzą, że lepiej jest, aby menedżerowie ds. bezpieczeństwa przyjęli założenie, że ich sieci obwodowe już zostały naruszone. „Specjaliści ds. zabezpieczeń muszą pogodzić się z faktem, że ich sieci mogą już być rozpracowane, tyle tylko, że jeszcze o tym nie wiedzą" — twierdzi O'Keeffe.

O'Keeffe twierdzi również, że w protokołach cyberbezpieczeństwa wszystkich z ponad 50 małych firm i przedsiębiorstw, które uwzględnił w swojej analizie, występowały luki umożliwiające hakerom uzyskanie dostępu do sieci poprzez jedną z drukarek, kamer, urządzeń przenośnych lub innych punktów końcowych z nią połączonych.

A zatem kluczem do utrzymania bezpieczeństwa sieci jest danie pracownikom IT narzędzi do wykrywania włamań i ochrony punktów końcowych, które można łatwo przeoczyć i które zdeterminowany przestępca wykorzysta do uzyskania dostępu. O'Keeffe podkreśla, że w razie włamania konieczne jest posiadanie solidnego, przywracającego bezpieczeństwo, rozwiązania do szybkiego reagowania i usuwania szkód.

Daniel Kalai, założyciel firm zajmujących się zarządzanymi usługami IT, do których należy firma oferująca zabezpieczenia dla biur domowych i małych firm pod nazwą Shieldly, przyznaje rację Shivaun Albright i Jasonowi O'Keeffe, że należy skupić się na zabezpieczeniu punktów końcowych sieci.[23] Uważa, że obecnie zamiast na zapobieganie zagrożeniom kładzie się nadmierny nacisk na przywracanie bezpieczeństwa. Nie zgadza się ze stwierdzeniem, że włamania do sieci nie da się uniknąć w dzisiejszym świecie cyfrowym.

„Niegdyś cyberbezpieczeństwo skupiało się na zapobieganiu" — twierdzi Kalai. „Jednakże obecnie na pierwszy plan wychodzi naprawa sytuacji. Smutny jest fakt, że ludzie tracą wiarę w narzędzia do zapobiegania. Można jednak wiele zrobić, aby zapobiec atakowi".

Cena awarii

Lepsze wykorzystanie urządzeń zabezpieczających, standardów i protokołów zabezpieczeń z pewnością poprawiłoby wyniki tych, którzy sumiennie wprowadzają programy cyberochrony, jednakże liczby z realnego świata pokazują, że występuje przepaść między planowaniem i realizacją.[23] I choć te same zagrożenia dotyczą wszystkich organizacji, problem nasila się w przypadku mniejszych firm, ponieważ nie dysponują one takimi środkami finansowymi, czasem i wyszkolonymi pracownikami, jak większe organizacje.[25]

Dlatego każdej osobie odpowiedzialnej za bezpieczeństwo danych firmy trzeba przypominać, o jaką stawkę toczy się gra: potencjalnie wielomilionowe straty niszczące wiarygodność i zaufanie w oczach klientów, procesy sądowe i znaczne zakłócenia w działalności.

Według raportu Ponemon Institute — niezależnej grupy zajmującej się badaniami nad bezpieczeństwem danych — przeciętne naruszenie zabezpieczeń danych kosztowało w 2017 roku 3,62 mln USD.[26] Badacze przeprowadzili rozmowy z przedstawicielami 419 firm z 13 krajów i stwierdzili, że każdy utracony lub skradziony rekord danych kosztuje przeciętnie 141 USD, a kwota ta szybko wzrasta przy coraz większym zakresie takich incydentów. Badanie wykazało wręcz, że w 2017 roku rozmiary przeciętnego naruszenia wzrosły o 1,8% w stosunku do roku ubiegłego.

Każda firma, która udostępniła swoje dane grupie Ponemon, odnotowała naruszenie spowodowane złośliwym lub przestępczym atakiem, usterką w systemie lub błędem ludzkim, przy liczbie rekordów danych objętych każdym incydentem wynoszącej od 2600 do prawie 100 000. Zidentyfikowanie i powstrzymanie naruszenia zajęło respondentom badania przeciętnie ponad dwa miesiące.

Złośliwe oprogramowanie jest coraz inteligentniejsze

Jonathan Griffin, starszy analityk bezpieczeństwa w HP Labs, twierdzi, że dostrzega więcej spektakularnych naruszeń, które przynoszą „szkody i straty na szokującym poziomie", czego przykładem jest zagrożenie z 2017 roku o nazwie NotPetya, które przyniosło szkody firmom w Stanach Zjednoczonych i w całej Europie, a którego głównym celem było, jak się wydaje, jedynie sianie zniszczenia.[27] Podobnie jak w przypadku wielu innych skutecznych ataków, zabezpieczenie przed wirusem WannaCry było dostępne przed wybuchem epidemii. Niestety wiele organizacji, dużych i małych, nie zainstalowało prostych poprawek oprogramowania, które zapobiegłyby włamaniu.

Jednakże skuteczne włamania nie są jedynie oznaką pogarszania się zabezpieczeń. W laboratorium HP zajmującym się złośliwym oprogramowaniem Griffin z zespołem zauważył, że w ciągu trzech ostatnich lat wzrósł rozmiar i złożoność szkodliwych programów. Programy te posiadają teraz znacznie lepszą funkcjonalność — porównywalną z fragmentami dobrze zaprojektowanego komercyjnego oprogramowania wysokiej jakości. Griffin twierdzi, że hakerzy-przestępcy i sponsorowani przez władze różnych państw są dobrze zorganizowanymi inżynierami, którzy stale doskonalą swoje rzemiosło i wykorzystują nowe narzędzia, takie jak uczenie maszynowe, które umożliwia systemom uczenie się z doświadczenia i samodoskonalenie bez specjalnego zaprogramowania.

> Rosnąca złożoność ataków w połączeniu z zaniedbywaniem cyberbezpieczeństwa zwiększa ryzyko dla sieci firmowych.

Rosnąca złożoność ataków w połączeniu z zaniedbywaniem cyberbezpieczeństwa zwiększa ryzyko dla sieci firmowych. Na szczęście, w opinii Jonathana Griffina, wielu informatyków i inżynierów z całego świata pracuje nad poprawą zabezpieczeń. Eksperci twierdzą, że organizacje wreszcie uświadamiają sobie, że wdrożenie zapory i oprogramowania antywirusowego to dopiero początek skutecznego programu, o wielu poziomach zabezpieczeń i z faktycznym nastawieniem na wykrywanie włamań.

Część 2:

Myśl jak da Vinci: dziedzina cyberbezpieczeństwa wymaga kreatywności

Aktualne i nowe zagrożenia dla cyberbezpieczeństwa wymagają połączenia sztuki z nauką.

Termin „człowiek renesansu” — na określenie osoby utalentowanej w wielu różnych dziedzinach — został ukuty z myślą o Leonardo da Vinci. Malarz, spod którego pędzla wyszyły takie dzieła, jak Ostatnia Wieczerza i Mona Lisa, był nie tylko artystą, lecz także inżynierem.
Jako inżynier wojskowości, którą to posadę zajmował przez prawie dwadzieścia lat, da Vinci wzmocnił system obrony Mediolanu, a jednocześnie udoskonalił i wynalazł nowe uzbrojenie. W ciągu swego życia opracował i udoskonalił także techniki budowy mostów oraz usprawnił elementy maszyn, takie jak przekładnie ślimakowe i koła zamachowe. Był ekspertem w dziedzinie hydrauliki, a nawet zaprojektował pojazd napędzany sprężyną.

Branża cyberbezpieczeństwa może się wiele nauczyć od mistrza. Aktualne i nowe zagrożenia dla cyberbezpieczeństwa wymagają połączenia sztuki z nauką — zwłaszcza w zakresie projektowania.

Osoby odpowiedzialne za bezpieczeństwo danych przedsiębiorstwa muszą uwzględnić wszystkie zasoby fizyczne i cyfrowe połączone z siecią organizacji — w którym miejscu sieci się znajdują, jak się łączą oraz jakie mają powiązania z innymi zasobami. Być może w realnym świecie jeszcze ważniejsze jest korzystanie przez pracowników podczas pracy z punktów końcowych, takich jak smartfony, drukarki i komputery przenośne. Ta kwestia powinna stanowić centralny element projektu zabezpieczeń i architektury.

Wszak najlepsze zabezpieczenia sieci działają tak, że użytkownicy nawet o nich nie wiedzą. Przydatna wskazówka, o której powinni pamiętać menedżerowie ds. bezpieczeństwa danych: korzystajcie z inteligentnych technologii, bądźcie niewidoczni, a zagrożenia niech mobilizują was do osobistego rozwoju.

Kluczowe jest aktywne monitorowanie

Allen Kent jest konsultantem ds. cyberbezpieczeństwa w NAES Corporation — firmie oferującej różne usługi dla różnych branż — od wytwarzania energii po produkcję masy papierniczej i papieru.[28] Kent nawet 24 razy w ciągu roku kontroluje elektrownie, poszukując luk w zabezpieczeniach. Jest wzywany do przeprowadzania audytów u producentów energii, właścicieli systemów przesyłowych i dystrybutorów, aby przygotować ich na zlecone przez władze federalne kontrole cyberbezpieczeństwa.

Takie audyty federalne są przeprowadzane co trzy do sześciu lat, w zależności od wpływu potencjalnego włamania na stabilność całej sieci elektroenergetycznej. Zaskakujący jest fakt, większość producentów energii elektrycznej uważa się za przedsiębiorstwa, w przypadku których włamanie nie miałoby większego znaczenia. O potencjalnie poważnym wpływie na stabilność sieci można mówić w przypadku wystąpienia problemu systemowego w tzw. ośrodku sterowania organu odpowiedzialnego za bilansowanie, który zarządza wahaniami podaży i popytu na energię elektryczną na poziomie regionów i całego kraju.

Zanim Kent poświęcił się pracy nad krytyczną infrastrukturą w przedsiębiorstwach produkujących energię elektryczną, zajmował się cyberbezpieczeństwem w sektorze bankowym i od wielu lat poszukuje sposobów na eliminację zagrożeń stwarzanych przez zorganizowane grupy przestępcze i wrogo nastawione państwa. Twierdzi, że pomimo znacznie większych w porównaniu z branżą finansową nakładów pracy, które muszą ponieść zakłady energetyczne, aby zapewnić zgodność ze standardami federalnymi, to cyberbezpieczeństwo w sektorze energetycznym stoi zasadniczo na dobrym poziomie. W jego opinii „Nie jest doskonałe (...) ale OK".

Jednym z największych wyzwań, które stoi przed Allenem Kentem, jest — jak twierdzi — nauczenie menedżerów, że nie istnieje wystarczające, gotowe rozwiązanie w zakresie cyberbezpieczeństwa, które można zainstalować i zapomnieć o całej sprawie. Uważa, że „zabezpieczenia należy stale monitorować". „Niestety większość mniejszych firm, niezależnie od branży, nie chce nikomu za to płacić. Są to ponoszone koszty bieżące bez żadnego zwrotu — dopóki nie dojdzie do zdarzenia, wobec którego takie koszty wynagrodzenia wydają się nieistotne".

Kent informuje przedsiębiorstwa, że swój program cyberbezpieczeństwa muszą zacząć od czterech działań: zainstalować zaporę i zadbać o jej prawidłową konfigurację; wdrożyć systemy monitorujące i filtrujące niebezpieczną lub podejrzaną zawartość w systemach e-mail i przeglądarkach internetowych; oddzielić chronione zasoby od tych, które nie wymagają takiego samego poziomu ochrony (u producenta energii elektrycznej na przykład komputery obsługujące elektrownię powinny być oddzielone od komputerów przetwarzających operacje biznesowe); wyznaczyć protokoły, pracowników i oprogramowanie do aktywnego monitorowania całości. Jest to standardowy model cyberbezpieczeństwa zwany obroną na obwodzie sieci: tworzy cyfrowe mury i systemy wykrywania włamań w celu powstrzymania intruzów.

Jednakże obecnie dostępne są nowe środki obrony, które umożliwiają menedżerom ds. cyberbezpieczeństwa podejmowanie znacznie bardziej ofensywnych działań. Jeszcze do niedawna eksperci uważali, że strategia zapobiegania pozwala wychwycić każde nowe zagrożenie pojawiające się w Internecie.
Jednakże dzisiejsze zautomatyzowane narzędzia do wykrywania włamań obserwują sieci w działaniu, aby poznać zasady przemieszczania się w nich danych, co pozwala wykrywać i powstrzymywać włamania, zanim urosną do niszczycielskich incydentów. Alarm może wyzwolić pozornie drobne zdarzenie, takie jak wysłanie z komputera przenośnego kilku gigabajtów danych poprzez sieć, która normalnie przesyła kilkaset megabajtów.

Cztery filary cyberbezpieczeństwa sieci:

01 Zainstaluj zaporę

02 Monitoruj i filtruj niebezpieczną lub podejrzaną zawartość

03 Oddziel chronione zasoby

04 Wyznacz protokoły

„Potrzebna jest zdolność do szybkiego wykrywania zagrożeń, odpowiedniego zareagowania, a następnie odzyskania sprawności w pełnej skali”.

VALI ALI
Współpracownik i główny technolog firmy HP

Wiele warstw ochrony przydaje się nie tylko w zimie

„Musimy tworzyć urządzenia, które mają kilka poziomów ochrony” — twierdzi Shivaun Albright z HP. „Określamy to mianem ochrony dogłębnej. Trzeba przyjąć do wiadomości fakt, że nie można ochronić się przed wszystkim. Potrzebna jest zdolność do wyszukiwania i wykrywania w urządzeniach nietypowych zachowań, które mogą wskazywać na atak”.

Idąc o krok dalej, współpracownik i główny technolog w firmie HP Vali Ali twierdzi, że funkcje zabezpieczeń i wykrywania muszą być wbudowane w urządzenia pracujące w sieci, a nie instalowane w późniejszym czasie.[29] W ostatnich latach postawiono na szybkie rozwijanie inteligentnego oprogramowania zabezpieczającego, które wykrywa zagrożenia w miarę ich pojawiania się, automatycznie zatrzymuje je i oczyszcza urządzenia ze złośliwych programów. Jednak aby działało optymalnie, musi być wbudowane i przezroczyste dla użytkownika, a także na tyle elastyczne, aby przeciwdziałać szerokiej gamie ataków.

Ponadto zakupy sprzętu IT wymagają dokładnego przemyślenia, aby znaleźć takie urządzenia, które będą spełniały swoje zadanie, a dodatkowo chroniły użytkowników i dane. „Zakup każdego urządzenia to decyzja wpływająca na bezpieczeństwo” — twierdzi Ali, dodając, że bezpieczeństwo wymaga połączenia technologii, świadomości, procesów i zarządzania.

Oprócz funkcji inteligentnego wykrywania, reagowania i uczenia się sieci i urządzenia muszą być odporne, aby szybko odzyskać sprawność po włamaniu. W opinii Vali Alego „atak z pewnością nastąpi”. „Potrzebna jest zdolność do szybkiego wykrywania zagrożeń, odpowiedniego reagowania, a następnie odzyskania sprawności w pełnej skali”.

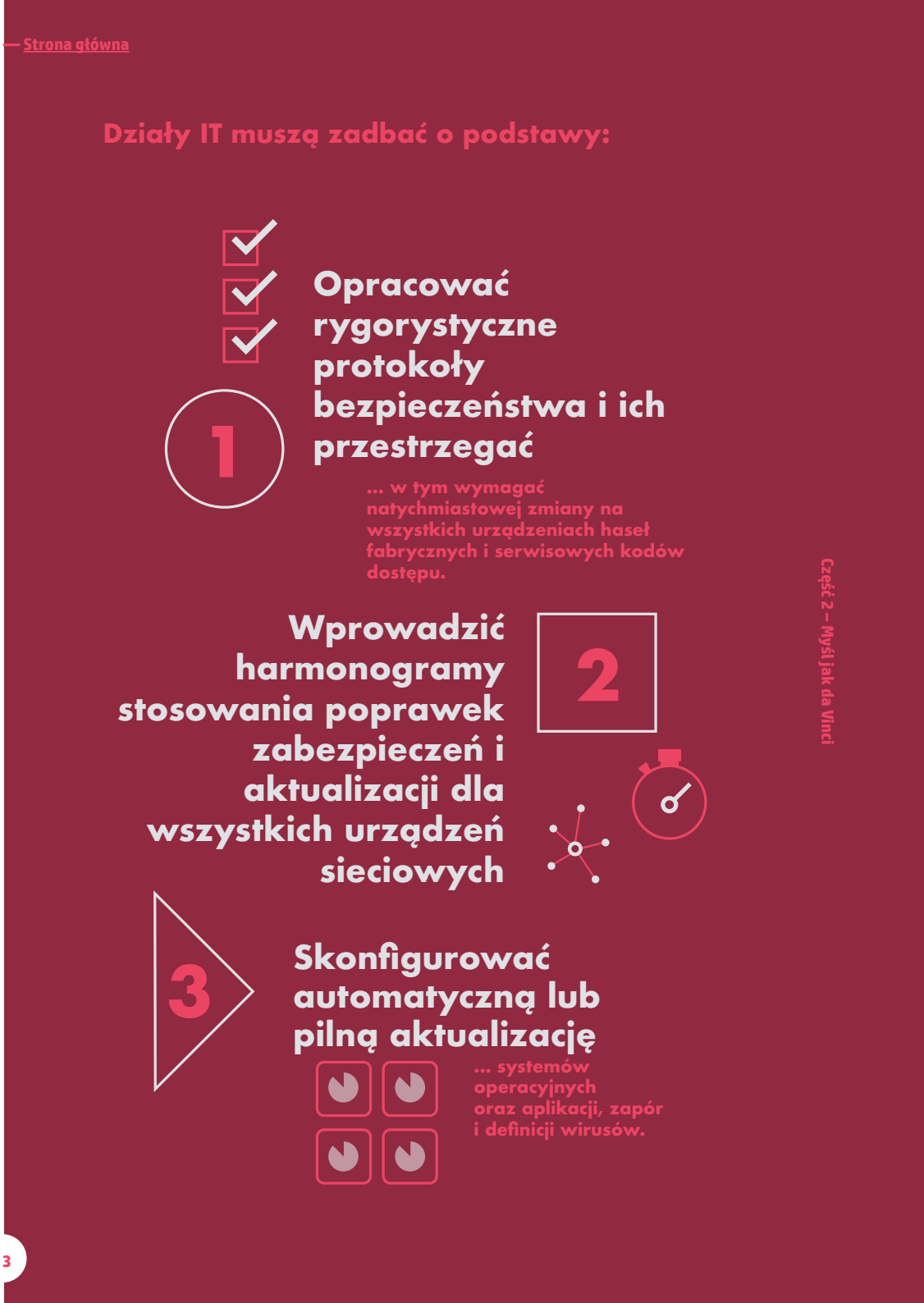
Zagrożenie na brzegu sieci

Niektóre organizacje o skali przedsiębiorstw posiadają odpowiednie zasoby, aby objąć ochroną obrzeża sieci. Jednakże wiele firm średniej wielkości i przedsiębiorstw nie zabezpieczyło wszystkich smartfonów, skanerów, drukarek i urządzeń IoT.[30] Shivaun Albright z firmy HP twierdzi, że jej rozmowy z klientami często ujawniają niespodziewany brak zainteresowania zabezpieczeniem punktów końcowych złożonych sieci.

„Zaskakujący jest dla mnie fakt, że choć wielu klientów doskonale zdaje sobie sprawę, że ich komputery, serwery i urządzenia sieciowe, takie jak przełączniki i routery, są zagrożone, to całkowicie lekceważy drukarki i inne urządzenia IoT" — mówi Albright. „Właśnie to chcemy zmienić poprzez uświadamianie i edukację — każdy punkt końcowy w sieci narażony na zagrożenie lub niezabezpieczony może stwarzać ryzyko dla całej infrastruktury".

Jednakże w pierwszej kolejności działy IT muszą zadbać o podstawy: 1) opracować rygorystyczne protokoły bezpieczeństwa i ich przestrzegać, w tym wymagać natychmiastowej zmiany na wszystkich urządzeniach haseł fabrycznych i serwisowych kodów dostępu; 2) wprowadzić harmonogramy stosowania poprawek zabezpieczeń i aktualizacji dla wszystkich urządzeń sieciowych; 3) skonfigurować automatyczną lub pilną aktualizację systemów operacyjnych oraz aplikacji, zapór i definicji wirusów. Firmy muszą także pilnować aktualności wykazu osób zatrudnionych i szybko cofać dostęp osobom, które już nie są pracownikami.

Ali twierdzi, że kluczowe jest także uwzględnienie aktualnych, nowych sposobów pracy w nowoczesnym biurze. Pracownicy w coraz większym stopniu oczekują możliwości pracy w dowolnym miejscu i czasie, a praca i zabawa często przeplatają się lub zamieniają miejscami — pracować można na plaży, a świętować w biurze. Zdaniem Vali Alego „biura przyszłości mają otwarte granice". „Jest to środowisko czynne przez całą dobę, 365 dni w roku, w którym życie osobiste przeplata się z pracą". Infrastruktura sieciowa, urządzenia i technologie sieciowe muszą dotrzymać kroku takim zmianom.



Analityk bezpieczeństwa Jonathan Griffin zauważa, że specjaliści ds. cyberbezpieczeństwa toczą nierówną wojnę, w której muszą być skuteczni przez cały czas, podczas gdy wystarczy, aby wróg był skuteczny jeden raz. Griffin podpowiada siedem najlepszych praktyk, które poprawią cyberbezpieczeństwo na dłuższą metę.

01 Wprowadź łatwe w realizacji procesy, które nie są zbyt złożone lub niejasne.

02 Przekazuj użytkownikom proste, spójne porady.

03 Stosuj w miarę możliwości uwierzytelnianie 2-składnikowe, gdyż hasła i zasady dotyczące haseł służbowych stwarzają wiele problemów.

04 Nie kupuj jedynie na podstawie ceny. Na podstawie zasad bezpieczeństwa podejmuj dobre decyzje o zakupie produktów zabezpieczających.

05 Przy wyznaczaniu w firmie zasad bezpieczeństwa nie zadowalaj się „pozorami bezpieczeństwa" i odhaczeniem punktów na liście. Upewnij się, że zabezpieczenia, za które płacisz, faktycznie zapewniają organizacji bezpieczeństwo.

06 Twórz bardziej sensowne raporty przez korzystanie z narzędzi analitycznych, które pokazują nie tylko ile ataków i wirusów zatrzymał system zabezpieczeń w danym miesiącu, lecz także ile z nich było nowych i unikatowych.

07 Producenci urządzeń IoT powinni wbudowywać zabezpieczenia w swoje produkty już od samego początku i zadbać o to, aby były one „bezpieczne z założenia".

Znaczenie edukowania pracowników

Współczesny brak ograniczenia ścianami biura zaostrza problem, który zawsze stwarzał zagrożenia dla bezpieczeństwa — ludzkie zachowanie. Pracownicy lekceważą uciążliwe protokoły bezpieczeństwa na rzecz wydajności pracy i często nie zdają sobie sprawy z faktu, że ich zachowanie online jest niebezpieczne. Z tego względu drobne, nieumyślne przypadki nieprzestrzegania zasad online są często źródłem awarii w sieciach, kradzieży własności intelektualnej lub przechwytywania wrażliwych danych klientów i przejęcia punktów końcowych przez botnety. „Zawsze znajdzie się ktoś, kto kliknie szkodliwe łącze w wiadomości e-mail" — twierdzi Shivaun Albright.

Jeden ze znanych producentów systemów przeciwdziałających złośliwemu oprogramowaniu donosi, że tylko 3% szkodliwych programów, z którymi ma do czynienia, bierze na cel usterki techniczne.[31] Oznacza to, że 97% hakerów korzysta z inżynierii społecznej, aby skłonić niczego niepodejrzewające ofiary do kliknięcia łącza w wiadomości e-mail typu phishing lub ujawnienia wrażliwych danych, takich jak hasła i numery rachunków bankowych.

Z tego względu kluczowe znacznie mają inicjatywy edukacyjne skierowane zarówno do personelu IT, w zakresie opracowywania i utrzymywania solidnych protokołów i procedur bezpieczeństwa danych, jak i pracowników niezwiązanych z IT, w zakresie ograniczania do minimum nieostrożnego zachowania użytkowników końcowych, które stwarza poważne zagrożenie dla bezpieczeństwa.

Kluczowe wskazówki, które należy uwzględnić w szkoleniach dla pracowników niezwiązanych z IT:

- Nie używaj tego samego hasła w różnych witrynach osobistych i służbowych.
- Nie pozostawiaj poufnych materiałów w drukarkach.
- Zablokuj komputer i urządzenia, gdy oddalasz się od nich.
- Używaj ekranów prywatności, które uniemożliwiają innym podgląd informacji na Twoim komputerze.
- Zdecydowanie nie klikaj łączy bez zastanowienia.

Jak projektanci, architekci i inżynierowie najlepszych systemów uwzględniają ludzkie zachowanie, aby ulepszyć sposoby zabezpieczania sieci i zasobów?

Zabezpieczenia przyszłości dostępne już dziś

Ali i analityk bezpieczeństwa Griffin wskazują na szereg innowacji firmy HP, które są już teraz powszechnie dostępne, a które nie obniżają wydajności pracy użytkowników, dzięki czemu pracownicy są mniej skłonni do ich ignorowania lub wyłączania.

Jedną z takich innowacji jest HP Secure — pakiet narzędzi do ochrony komputerów, który obejmuje narzędzia Sure View, Sure Click i Sure Start.

HP Sure View to zintegrowany ekran prywatności dla komputerów, który uniemożliwia osobom postronnym odczyt danych wyświetlanych na monitorach użytkowników. „To znakomite zabezpieczenie" — twierdzi Griffin. „Jest łatwe w użyciu, użytkownicy wiedzą, że działa i jak działa".

HP Sure Click to egzekwowane sprzętowo zabezpieczenie przeglądarek internetowych, które odizolowuje złośliwe oprogramowanie na maszynie wirtualnej, aby nie zainfekowało systemu. „Ile razy kliknęliście łącze, zaraz potem stwierdzając: <<Kurczę, nie trzeba było klikać>>?" — mówi Ali. „Po zastosowaniu narzędzia Sure Click złośliwe oprogramowanie nie ma wglądu w komputer użytkownika. W razie przypadkowego pobrania złośliwego oprogramowania wystarczy zamknąć kartę, aby się go pozbyć. To znakomite rozwiązanie, ponieważ nie prosimy użytkowników o zmianę zachowania, aby mogli surfować bezpieczniej".

Takie rozwiązanie w zakresie cyberbezpieczeństwa, które pomija działania użytkowników, umożliwi w przyszłości ograniczenie znacznego wpływu czynnika ludzkiego we włamaniach do sieci.

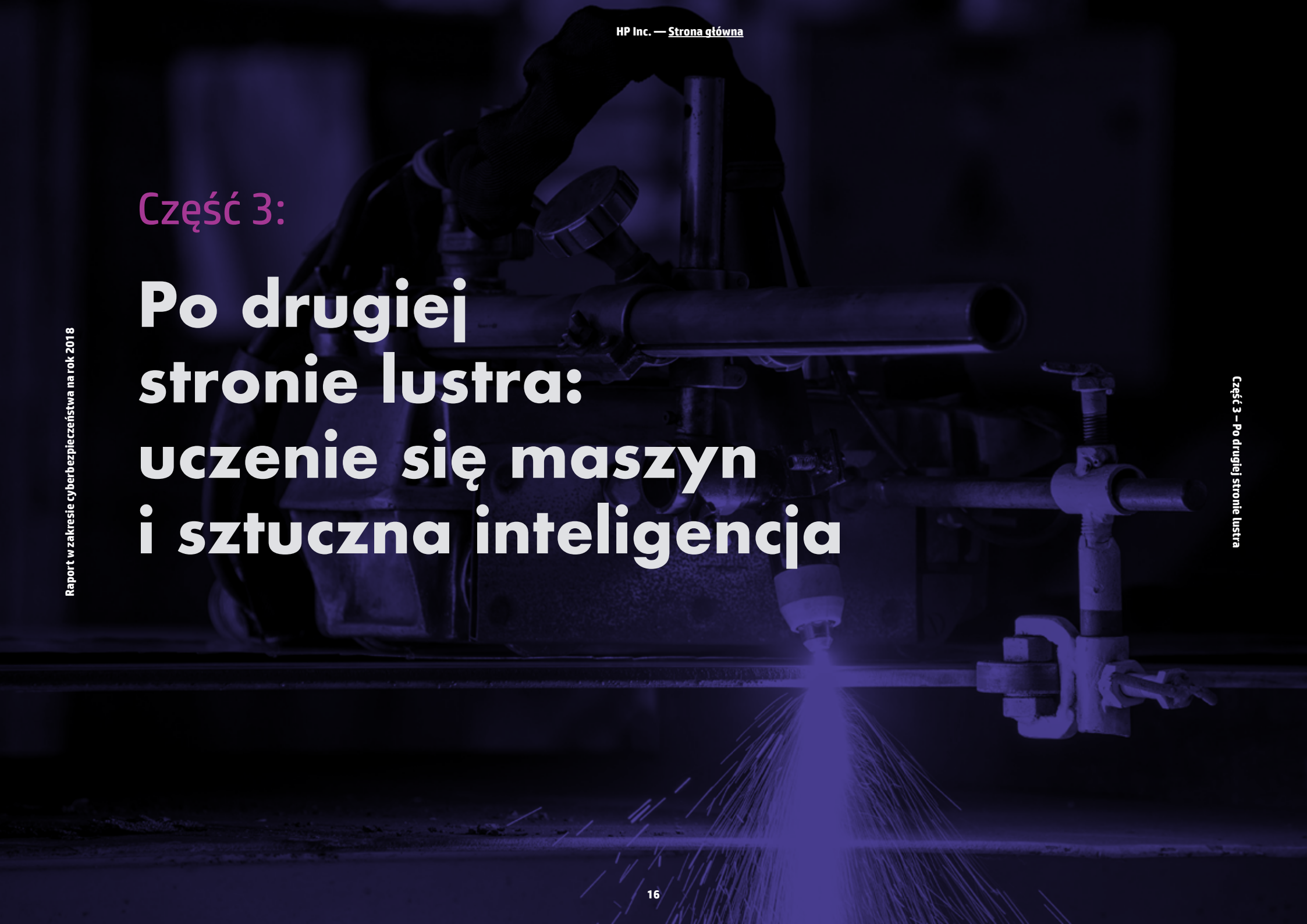
HP Sure Start weryfikuje ochronę przed złośliwym oprogramowaniem poprzez analizę oprogramowania sprzętowego BIOS — najbardziej podstawowego elementu systemu operacyjnego komputera. Obszar ten coraz częściej staje się celem ataków, ponieważ wykrycie włamania w nim jest bardzo trudne. Bez właściwych zabezpieczeń złośliwe oprogramowanie zainstalowane w systemie BIOS jest niewidoczne, umożliwiając intruzowi stałą obecność w sieci. Badanie Data Breach Investigations Report firmy Verizon z 2016 roku wykazało, że takie podejście jest coraz częściej przyjmowane przez intruzów: Analitycy stwierdzili wzrost o 132% liczby incydentów ukierunkowanych na notebooki i komputery stacjonarne w stosunku do ubiegłego roku.[32]

HP Sure Start uniemożliwia oszustom umieszczanie złośliwego oprogramowania w systemie BIOS sieci. Przy uruchamianiu komputera wbudowana funkcja sprawdza czystość systemu BIOS. W razie stwierdzenia infekcji narzędzie HP Sure Start automatycznie przywraca czystą wersję kodu, bez interwencji użytkownika czy personelu IT. W opinii Vali Alego „jest to z założenia bezpieczne rozwiązanie".

Zintegrowany ekran prywatności **HP Sure View** jest rozwiązaniem opcjonalnym i musi zostać skonfigurowany przy zakupie. Dostępne tylko w wybranych notebookach firmy HP.

Aplikacja **HP Sure Click** jest dostępna na wybranych platformach HP i obsługuje przeglądarki Microsoft® Internet Explorer i Chromium™. Sprawdź tutaj wszystkie zgodne platformy, które są aktualnie dostępne.

Rozwiązanie **HP Sure Start Gen4** jest dostępne w produktach HP Elite i HP Pro 600 wyposażonych w procesory Intel® 8. generacji lub procesory AMD.



Część 3:

Po drugiej stronie lustra: uczenie się maszyn i sztuczna inteligencja

Sztuczna inteligencja poprzez uczenie się maszyn zaczyna pomagać w utrzymaniu bezpieczeństwa naszego otoczenia cyfrowego.

Aktualnie stosowane najlepsze praktyki w zakresie cyberochrony obejmują technologie wielowarstwowe, logowanie biometryczne i monitorowanie sieci, w połączeniu z właściwym edukowaniem pracowników w zakresie bezpieczeństwa online, natomiast sztuczna inteligencja poprzez uczenie maszynowe zaczyna pomagać w utrzymaniu bezpieczeństwa naszego cyfrowego otoczenia.

Kolejna innowacja firmy HP chroni podatne na zagrożenia drukarki połączone z siecią jako punkty końcowe. Opracowane w HP Labs i już dostępne narzędzie HP Connection Inspector to inteligentne, wbudowane zabezpieczenie, które poznaje normalne zachowanie drukarki w sieci, a następnie wykrywa podejrzane zmiany. Gdy wykryje nietypowe dane wychodzące, powiadamia administratorów, zamyka podejrzaną komunikację, a następnie wymusza samonaprawcze ponowne uruchomienie w celu usunięcia złośliwego oprogramowania i powstrzymania ataku.

Te innowacje sprawiają, że Allen Kent z NAES staje się ostrożnym optymistą. Czeka na dzień, gdy technicy będą mogli podłączyć do sieci urządzenie, które poszukuje zagrożeń zawartych w strumieniach przesyłanych danych, natychmiast zamyka wymianę danych w razie wykrycia włamania, a następnie analizuje szczegóły ataku w celu wywnioskowania, jak podobny atak wyglądałby od samego początku. „Urządzenie wyposażone w sztuczną inteligencję, które monitoruje wszystko i automatycznie powstrzymuje zagrożenia, gdy tylko się pojawią — to byłoby wspaniałe" — podsumowuje Allen Kent.

Objęcie urządzeń IoT parasolem ochrony

Wbudowanie procesorów i funkcji dostępu do Internetu w termostaty, czujniki ruchu, systemy oświetlenia i inne sprawia, że budynek biurowy może samodzielnie znaleźć pokaźne oszczędności energii na podstawie stopnia zajętości pomieszczeń, pory dnia, a nawet pogody.[33] Turbina wiatrowa zgłasza menedżerom nadmierne drgania przekładni w jej gondoli i konieczność zwrócenia na nie uwagi[34]. Silnik odrzutowy i komputer pokładowy komercyjnego samolotu współpracują ze sobą, dokonując chwilowych zmian zmniejszających zużycie paliwa i skracających czas odchylenia od właściwego kursu.[35]

Takie inteligentne urządzenia trafiają także do naszych domów w postaci inteligentnych termostatów, lodówek, żarówek i bazujących na sztucznej inteligencji asystentów cyfrowych.

W przyszłości pojawią się także inteligentne protezy i implanty siatkówkowe, z wbudowanymi mikroskopijnymi procesorami i dostępem do Internetu. Co się stanie, jeśli hakerzy wezmą je na cel?

„Pomyślmy, co by się stało, gdyby oprogramowanie sprzętowe implantu siatkówkowego lub protezy nogi wydrukowanej na drukarce 3D stało się celem ataku lub zostało zainfekowane przez oprogramowanie typu ransomware" — zastanawia się Vali Ali z firmy HP. „Jak to by wyglądało? Co zrobiliby ludzie, którzy nagle utracili wzrok i dostali wiadomość o treści: <<Zapłać, a odzyskasz wzrok>>?".

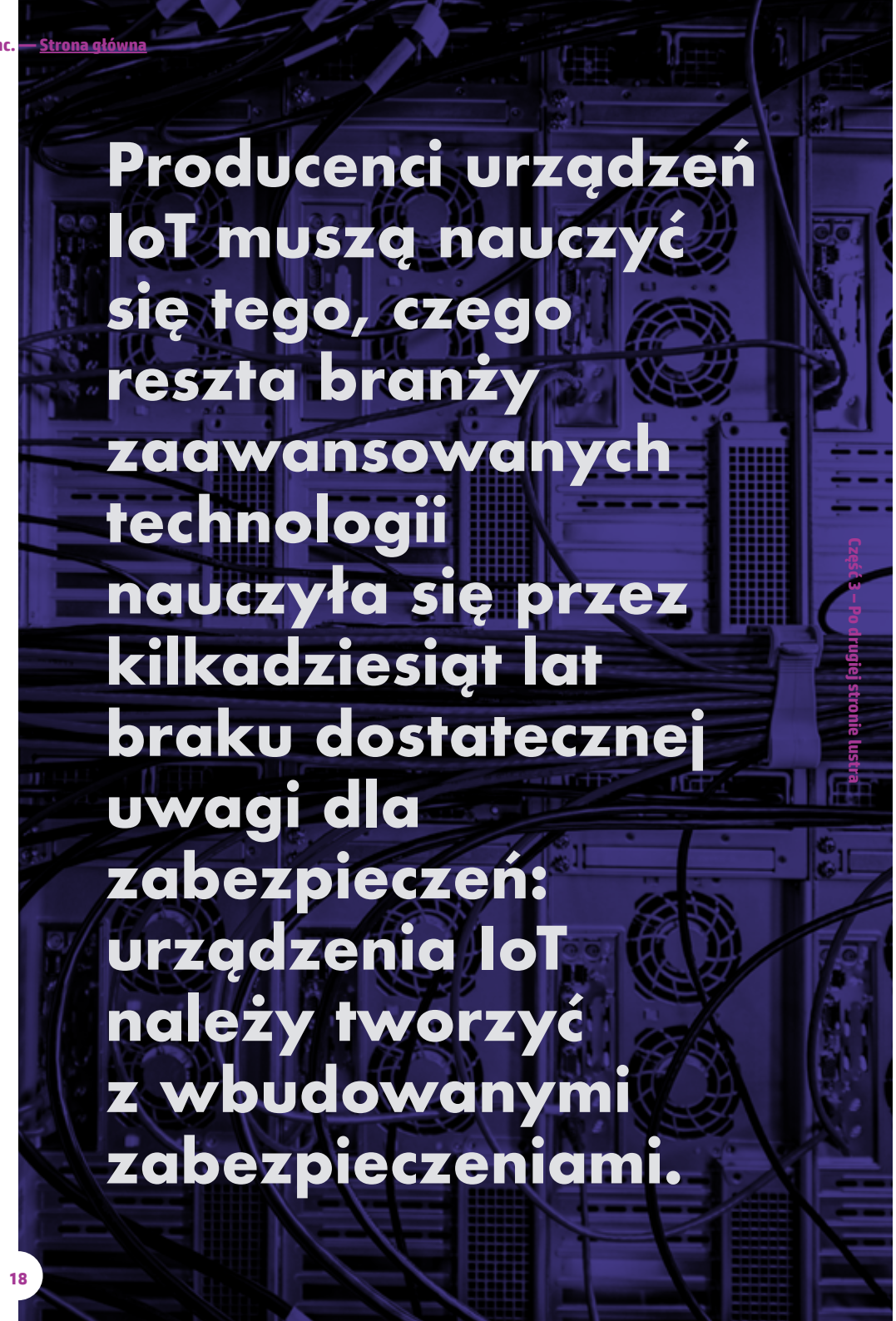
Właśnie tu dochodzi do głosu odporność, która umożliwia zainfekowanemu urządzeniu szybkie usunięcie złośliwego oprogramowania i powrót do trybu online w czystym stanie. Według Allego „z chwilą zainfekowania implantu siatkówkowego złośliwym oprogramowaniem lub oprogramowaniem typu ransomware wystarczyłoby mrugnąć oczami, aby usunąć je i odzyskać wzrok".

Jak twierdzi Griffin, aby to osiągnąć, producenci urządzeń IoT muszą nauczyć się tego, czego reszta branży zaawansowanych technologii nauczyła się przez kilkadziesiąt lat braku dostatecznej uwagi dla zabezpieczeń: urządzenia IoT należy tworzyć z wbudowanymi zabezpieczeniami. Jeśli zatem inteligentna żarówka zostanie zainfekowana złośliwym oprogramowaniem, powinna być w stanie wyłączyć się, uruchomić ponownie, usunąć obcy kod i ponownie włączyć.

Łatwość obsługi chroni przed złym zachowaniem

„Nie do zaakceptowania jest sytuacja, że wkładam klucz do zamka i muszę czekać na wiadomość SMS w celu weryfikacji, że to ja próbuję się dostać do własnego domu" — stwierdza Griffin. „Technologia nie może utrudniać życia".

W celu rozwiązania tego znanego problemu inżynierowie od lat pracują nad usprawnieniem logowania, a techniki komputerowego rozpoznawania twarzy, biometrycznego rozpoznawania linii papilarnych lub siatkówki powoli zaczynają zastępować tradycyjne hasła alfanumeryczne.[36]



„To jest wyścig zbrojeń i zawsze trudno jest stwierdzić, gdzie hakerzy uderzą w następnej kolejności”.

JONATHAN GRIFFIN,
starszy analityk bezpieczeństwa w HP Labs

Kolejne rozwiązanie, czyli technologia HP WorkWise, to darmowa aplikacja dostępna w sklepie Google Play, która tworzy łącze kryptograficzne między smartfonem pracownika i komputerem. Dzięki takiemu łączu komputer wie, kiedy użytkownik odszedł od komputera, i może automatycznie zablokować się, aby inni nie mieli do niego dostępu. Po powrocie użytkownika komputer rozpoznaje go i loguje z powrotem, bez potrzeby podawania hasła. Ta technologia stanowi przykład zasady „nie przeszkadzać”, gdyż pomaga użytkownikom w zachowaniu bezpieczeństwa bez potrzeby wykonywania z ich strony jakichkolwiek dodatkowych czynności.

„Istnieją dwa rodzaje technologii” — mówi Vali Ali. „Takie, których ludzie chcą używać, oraz uciążliwe, których ludzie muszą używać. Jeśli ludzie będą zmuszani do korzystania z uciążliwych zabezpieczeń, ostatecznie znajdą sposób, by je obejść”.

Uczenie maszynowe to miecz obosieczny

Czasy, w których skanowanie w poszukiwaniu złośliwego oprogramowania było głównym narzędziem obrony przed hakerami, należą do przeszłości.[37] Oprogramowanie przeciwdziałające złośliwemu oprogramowaniu musi być aktualizowane o znany szkodliwy kod, aby wiedziało, czego szukać. Takie rozwiązanie nie jest przydatne, gdy w sieci pojawia się nowy szkodliwy kod, co ma miejsce częściej niż przypuszczają badacze.

Po stronie obrońców bezpieczeństwa zaczyna się wykorzystywać dane i uczenie maszynowe do zautomatyzowanej analizy sieci, która weryfikuje dane ze stałego strumienia przepływającego do, z lub poprzez sieć firmową w poszukiwaniu anomalii. Takie funkcje obliczeniowe będą w przyszłości poszukiwać na przykład skoków aktywności procesora, mogących sygnalizować początek problemu. Po stronie hakerów uczenie maszynowe może być wykorzystywane do automatyzacji sondowania, skanowania i kontrolowania sieci.

Jonathan Griffin z firmy HP twierdzi, że uczenie maszynowe i inne formy sztucznej inteligencji już dają przewagę obrońcom bezpieczeństwa. Ostrzega jednak, że narzędzia takie jak uczenie maszynowe nie stanowią panaceum na wszystko. Uczenie się maszyn może wręcz z dużym prawdopodobieństwem stworzyć nowy kierunek ataków dla hakerów, którzy poszukują słabych punktów w opartych na nim zabezpieczeniach i sami wykorzystują uczenie maszynowe/sztuczną inteligencję do projektowania tańszych i skuteczniejszych ataków. „To jest wyścig zbrojeń i zawsze trudno jest stwierdzić, gdzie hakerzy uderzą w następnej kolejności” — stwierdza Griffin.

Czy sztuczna inteligencja rozwiąże problem cyberbezpieczeństwa, czy też go nasili?

W przyszłości zaawansowane algorytmy stojące za rozwiązywaniem problemów poprzez uczenie maszynowe rozwiną się w solidniejsze systemy sztucznej inteligencji. Hakerzy dysponujący odpowiednimi zasobami będą wykorzystywać sztuczną inteligencję do sondowania i atakowania sieci. Zaawansowane technologie pozwolą im udoskonalić metody oparte na inżynierii zachowań, aby ataki z wykorzystaniem techniki phishingu i złośliwego oprogramowania nie dały się odróżnić od legalnych wiadomości e-mail i witryn internetowych. Hakerzy i obrońcy bezpieczeństwa będą wykorzystywać sztuczną inteligencję do przekierowania strumieni danych w sieci podczas ataków DDoS w celu nasilenia lub złagodzenia szkód.

Według Alego „będziemy żyć w świecie inteligentnych ataków wykorzystujących sztuczną inteligencję". „Mogło już do tego dojść, ale system był na tyle inteligentny, że nikt się o tym nie dowiedział".

W przyszłości inżynierowie powinni rozwinąć możliwości dynamicznego uczenia w ramach sztucznej inteligencji na tyle, aby systemy obronne mogły korzystać z danych historycznych i aktualnych trendów do przewidywania ataków, ich udaremniania lub powstrzymywania i ewentualnie do namierzania miejsc przebywania przestępców.

Na chwilę obecną producenci myślący o przyszłości dopiero zaczynają skłaniać się ku produkcji urządzeń, o jakich marzy Allen Kent z NAES: sztuczna inteligencja w pudełku. Pierwszym krokiem jest umieszczenie zabezpieczeń w sercu produktów już na samym początku procesu projektowania.

Zwycięstwo w niekończącej się walce ze złem

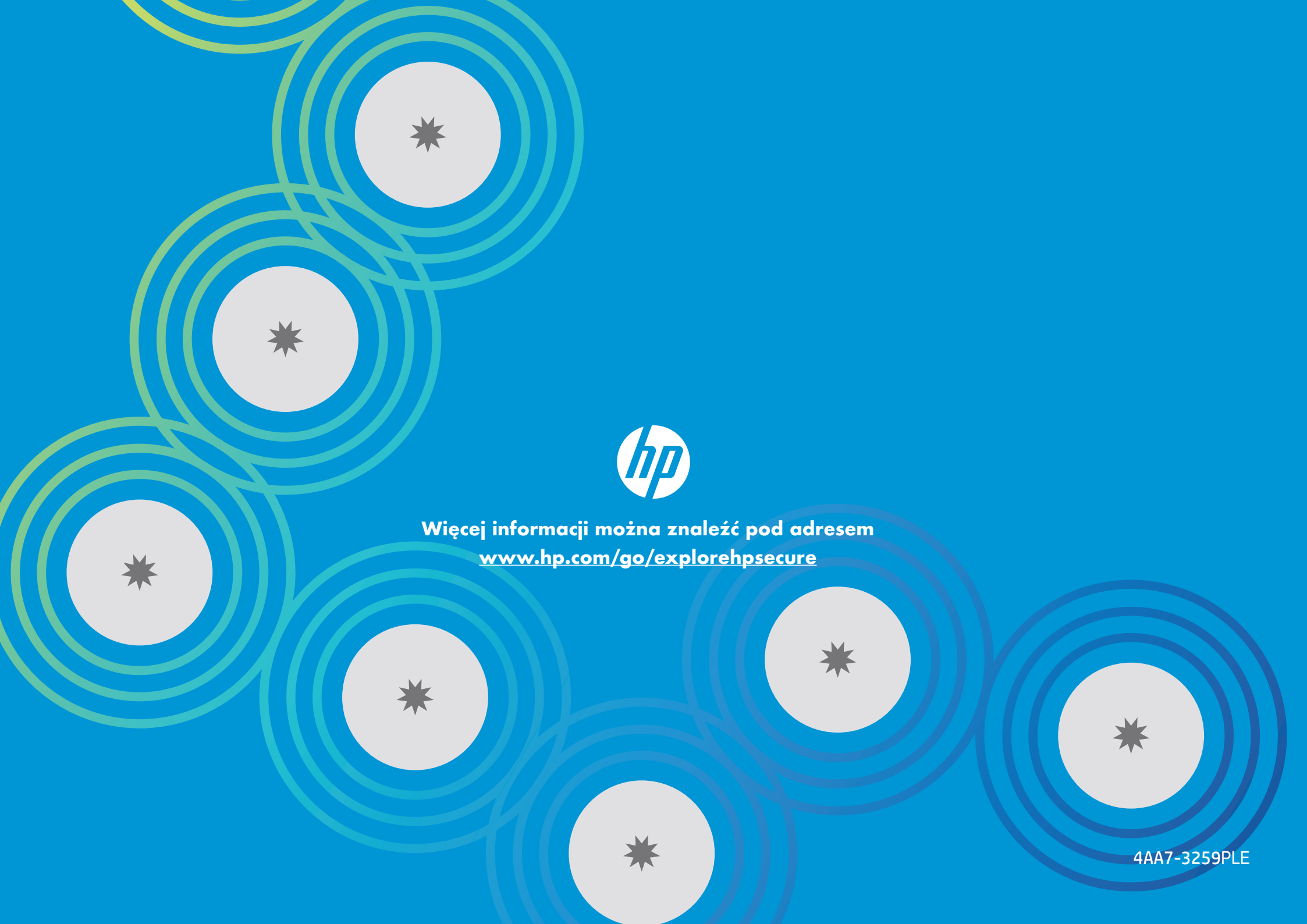
Cybernetyczna wojna między tymi dobrymi i tymi złymi trwa na dobre, z różnymi rezultatami w różnych branżach. Wobec faktu, że elementy przestępcze i polityczne dokładają wszelkich starań, aby spenetrować sieci i zakłócić ich działanie, stawka jest ogromna, a zagrożenia nie znikną na nasze życzenie.

> Odbywa się nieustanna walka dobra ze złem. To walka, której my, ci dobrzy, nie możemy przegrać. Nie wolno nam jej przegrać. W HP podjęliśmy zobowiązanie: Tej walki nie przegramy.

Ochrona niezawodności systemów cyfrowych umożliwiających pracę krytycznej infrastruktury i organów władzy państwowej, a także dużych i małych firm, ma dzisiaj kluczowe znaczenie dla codziennego życia, zarobkowania i społeczeństwa. „Według nas świat ma swoje złowrogie oblicze, ale jest w nim też dobroć" — twierdzi Vali Ali z firmy HP. „Odbywa się nieustanna walka dobra ze złem. To walka, której my, ci dobrzy, nie możemy przegrać. Nie wolno nam jej przegrać. W HP podjęliśmy zobowiązanie: Tej walki nie przegramy".

Przypisy końcowe

1. Robotics Business Review, „Robot Investments Weekly: AI, Industrial Automation, Mobility Market Drive Spending”, https://www.roboticsbusinessreview.com/financial/robot-investments-weekly-ai-industrial-automation-mobility-market-drive-spending/ (dostęp uzyskano 26 lutego 2018 r.)
2. TechEmergence, „Machine Learning Drug Discovery Applications – Pfizer, Roche, GSK, and More”, https://www.techemergence.com/machine-learning-drug-discovery-applications-pfizer-roche-gsk/ (dostęp uzyskano 26 lutego 2018 r.)
3. Popular Mechanics, „The Surgeon Will Skype You Now”, https://www.popularmechanics.com/science/health/a19208/the-surgeon-will-skype-you-now/ (dostęp uzyskano 26 lutego 2018 r.)
4. CFO, „Cyber Attacks Can Cause Major Stock Drops”, http://ww2.cfo.com/cyber-security-technology/2017/04/cyber-attacks-stock-drops/ (dostęp uzyskano 26 lutego 2018 r.)
5. Kaspersky, „Cyberthreat Real-Time Map: Local infections in the last week”, https://cybermap.kaspersky.com/stats/ (dostęp uzyskano 26 lutego 2018 r.)
6. Anti-Phishing Working Group, „Global Phishing Survey”, https://apwg.org/resources/apwg-reports/domain-use-and-trends
7. G DATA Security Blog, „Malware Trends 2017”, https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017
8. Digital Attack Map, „What is a DDoS Attack?” http://www.digitalattackmap.com/understanding-ddos/
9. Digital Attack Map, „Top Daily DDoS Attacks Worldwide”, http://www.digitalattackmap.com/
10. U.S. Department of Defense, „‘Terabyte of Death’ Cyberattack Against DoD Looms, DISA Director Warns”, https://www.defense.gov/News/Article/Article/1414146/
11. HP, „HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack”, http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676
12. Greenfield Daily Reporter, „Hospital Falls Victim To Hacker Attack; No Patient Records Compromised”, http://www.greenfieldreporter.com/2018/01/12/hospital-falls-victim-to-hacker-attack-no-patient-records-compromised-officials-said/
13. Black Hills Pioneer, „Belle Fourche City Servers Hacked”, http://www.bhpioneer.com/local_news/belle-fourche-city-servers-hacked/article_7254ad36-f576-11e7-8ed7-e31c3ee0da87.html
14. Columbia Daily Herald, „MCPS Experiences Cyber Attack”, http://www.columbiadailyherald.com/news/20180105/mcps-experiences-cyber-attack
15. Bloomberg Technology, „‘It Can’t Be True.’ Inside the Semiconductor Industry’s Meltdown”, https://www.bloomberg.com/news/articles/2018-01-08/-it-can-t-be-true-inside-the-semiconductor-industry-s-meltdown
16. The Economic Times of India, „3.2 Million Debit Cards Compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis Worst Hit”, (Paywall) https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms
17. CNBC, „Virtual Extortion a Big Business for Cyber Criminals”, https://www.cnbc.com/2016/02/17/ransomware-is-targeting-us-companies-of-all-sizes.html
18. Cybersecurity Ventures, „Cybercrime Report”, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
19. Wywiad telefoniczny z Jasonem O’Keeffe, HP (14 grudnia 2017 r.)
20. Wywiad telefoniczny z Shivaun Albright, HP (15 grudnia 2017 r.)
21. CoinDesk, „Botnet Infects Half a Million Servers to Mine Thousands of Monero”, https://www.coindesk.com/botnet-infects-half-million-servers-mine-thousands-monero/
22. Wywiad telefoniczny z Danielem Kalai, Shieldly (10 stycznia 2018 r.)
23. Financial Times, „‘Essential’ services face fines for poor cyber security”, (Paywall) https://www.ft.com/content/f2faf8cc-7b79-11e7-ab01-a13271d1ee9c
24. Houston Chronicle, „Consequences of Poor Security in a Company”, http://smallbusiness.chron.com/consequences-poor-security-company-70227.html
25. IBM and Ponemon Institute, „2017 Ponemon Cost of Data Breach Study”, https://www.ibm.com/security/data-breach
26. Wywiad telefoniczny z Jonathanem Griffinem, HP (21 grudnia 2017 r.)
27. Wywiad telefoniczny z Allenem Kentem, NAES (15 stycznia 2018 r.)
28. Wywiad telefoniczny z Valim Ali, HP (15 grudnia 2017 r.)
29. Keeper Security, „2017 State of Cybersecurity in Small & Medium-sized Businesses”, https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html
30. Digital Guardian, „Social-Engineering Attacks: Common Techniques & How to Prevent an Attack”, https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
31. Verizon, „2016 Data Breach Investigations Report”, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
32. Intel, „Reduce Energy Costs and Carbon Footprint with Smart Building Management”, https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/iot-ecs-tatung-reduce-carbon-footprint-solution-brief.pdf
33. Industrial Internet Consortium, „The Benefits of IoT Analytics for Renewable Energy”, https://www.iiconsortium.org/case-studies/ParStream_Envision_Energy_Case_Study.pdf
34. Aviation Week, „Internet Of Aircraft Things: An Industry Set To Be Transformed”, http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed
35. Global Cyber Alliance, „How Biometrics Can Replace Passwords”, https://www.globalcyberalliance.org/how-biometrics-can-replace-passwords.html
36. Wall Street Journal, „The Limits of Antivirus Software”, (Paywall) https://www.wsj.com/articles/the-limits-of-antivirus-software-1505700000



Więcej informacji można znaleźć pod adresem
www.hp.com/go/explorehpsecure

4AA7-3259PLE