Internet. Hacking

Wstęp

Wstęp

Termin hacking jest używany od połowy XX w. Początkowo wiązał się głównie ze swoistymi eksperymentami intelektualnymi oraz zastosowaniem kreatywnych sposobów rozwiazywania problemów technicznych. W latach 80. XX w. terminem hacking zaczęto też oznaczać złośliwą ingerencję, a słowem hacker „cyfrowego intruza".

W tym tomie hacking jest rozpatrywany z różnych perspektyw, jako: przestępstwo, incydent cyberbezpieczeństwa, eksplorowanie i modyfikowanie systemów technicznych, społecznych i biologicznych, a najogólniej – jako przełamywanie zabezpieczeń.

Historia pokazuje, że gdy pojawia się przełomowa zawodność zabezpieczeń „przemija postać świata". Druga dekada XXI w. przyniosła symptomy gwałtownego poszerzania pól przewagi sztucznej inteligencji nad człowiekiem w określaniu co jest istotne. Wystawiła też na ciężkie próby przewagę traktowania prawa jako „wędzidła dla siły" w konfrontacji z reżimami autorytarnymi. Zatem przełamywanie zabezpieczeń określane jako hacking wymaga refleksji. Mogą w niej być pomocne wyniki badań prowadzonych w 2022 r. przez ekspertów skupionych wokół Naukowego Centrum Prawno-Informatycznego.

Część I publikacji dotyczy problemów cyberbezpieczeństwa, ataków i przeciwdziałania cyberprzestępczości. W części II podejmowane są kwestie danych osobowych i ich ochrony przed naruszeniami. Zagadnienia sztucznej inteligencji i tożsamości cyfrowej rozważane są w części III. Ostatnia, czwarta część monografii odnosi się do wzmacniania kompetencji cyfrowych i cyberhigieny.

Rozwój technologii prowadzi do ograniczania roli osoby fizycznej przy jednoczesnym wzroście znaczenia powiązanej z nią „osoby cyfrowej" (*digital person*), co sprawia, że krytycznym problemem jest zapewnienie zaufania w systemach teleinformatycznych (*M. Kutyłowski*). W związku z wykorzystywaniem technologii informacyjno-komunikacyjnych w różnych sekto-

rach, brak zaufania do cyberbezpieczeństwa produktów, usług czy procesów skutkować będzie utratą zaufania do osób wykonujących określone zawody (medyczne) czy podmiotów prowadzących określoną działalność opartą na zaufaniu (*K. Świtała*). Zaufanie do nowych technologii zwiększać może certyfikacja (*A. Besiekierska*, *T. Chomicki*, *K. Grondys*, *M. Rawski*, *P. Drobek*), audyty, akty normatywne (*B. Fischer*) czy przyjęte procedury oceny profili ryzyka dostawców oparte na zróżnicowanych przesłankach (*M. Wysocki*). Zapewnienie bezpiecznych i wygodnych usług cyfrowych obywatelom innych krajów, powiązane z uznaniem ich wirtualnego pobytu (e-rezydencji), prowadzić może do „rekrutacji nowych e-obywateli", choć z drugiej strony rozwój e-usług oraz zależność od infrastruktury teleinformatycznej zwiększa ryzyka związane z cyberatakami (*P. Kuzior*).

Szczególne wyzwania wiążą się z ochroną danych osobowych w procesach komunikacyjnych (*M. Sakowska-Baryła*), z prawnymi i technicznymi aspektami monitoringu (*A. Zubrycka*, *M. Jakubik*, *K. Witas*), wykorzystaniem danych biometrycznych (*M. Świerczyński*) i zagrożeniami prywatności przez inteligentne urządzenia pomiarowe (*M. Szyrski*). Trudne w praktyce okazuje się urzeczywistnianie praw osób, których dane są przetwarzane i realizacja będących refleksem tych praw obowiązków podmiotów przetwarzających, w tym zwłaszcza obowiązku informacyjnego (*M. Kuźmicz*, *A. Zubrycka*).

Referowane w tej książce badania prowadzą do konstatacji, że mierzymy się z „wyścigiem cyber zbrojeń", zaś na pole bitwy składają się nie tylko infrastruktura teleinformatyczna (operacje CyberOps), ale także „podłączeni" do tej infrastruktury ludzie jako „mózgi realizujące procesy poznawcze" (operacje InfoOps) (*R. Kasprzyk*). Krajobraz zagrożeń bezpieczeństwa dla obywateli, w tym ich elektronicznej tożsamości (*K. Czaplicki*, *M. Badowski*), organizacji i państw zmienia sztuczna inteligencja (*J. Cytowski*). Sztuczna inteligencja i cyberbezpieczeństwo mają jednak wielowymiarową relację i szereg współzależności. W kontekście cyberprzestępczości sztuczna inteligencja może być wykorzystywana zarówno w klasycznych atakach jako środek wspomagający i ułatwiający, jak również może być kluczowym celem ataków (*A. Gryszczyńska*). Wagę regulacji normatywnej w tym obszarze oraz destrukcyjne skutki ataków adwersarskich poddano analizie w odniesieniu do technologii medycznych (*J. Greser*). Wykorzystanie technologii medycznych (czujników, IoT), AI i big data sprawia, że możliwe staje się określanie sposobu dokonywania wyborów przez ludzi, a uzyskanie dostępu do „ludzkiego systemu operacyjnego" umożliwi manipulowanie nimi (hakowanie), zwiększając podatność na reklamę czy propagandę (*G. Tokarska*).

Wobec nowych zagrożeń, na które narażone są w szczególności dzieci i młodzież, budowanie kompetencji cyfrowych, w tym umiejętności praktycznych z zakresu cyberhigieny powinno zostać rozpoczęte na wczesnych etapach edukacji, przy wsparciu nowoczesnych, multimedialnych narzędzi, w tym edu-

kacyjnych gier wideo (*K. Radomiński*) czy infografiki (*W. Święcicki*). Zabezpieczenie zbiorów danych przed zagrożeniami, dostępem osób nieupoważnianych, wyciekiem lub utratą danych stały się wyzwaniami również dla uczelni (*B. Zbarachewicz*). Wielość ataków hakerskich na szkoły wyższe, a równocześnie znaczenie kompetencji cyfrowych ich absolwentów dla zapewniania cyberbezpieczeństwa w podmiotach, w których po studiach podejmują pracę, motywuje do zwrócenia szczególnej uwagi na problem podnoszenia kompetencji cyfrowych społeczności akademickich (*G. Szpor*).

Problemami badawczymi poprzednich jedenastu tomów serii Internet były: Ochrona wolności, własności i bezpieczeństwa, red. *G. Szpor*, Warszawa 2011; Prawno-informatyczne problemy sieci, portali i e-usług, red. *G. Szpor*, *W.R. Wiewiórowski*, Warszawa 2012; Cloud computing. Przetwarzanie w chmurach, red. *G. Szpor*, Warszawa 2013; Publiczne bazy danych i big data, red. *G. Szpor*, Warszawa 2014; Internet rzeczy. Bezpieczeństwo w Smart city, red. *G. Szpor*, Warszawa 2016; Strategie bezpieczeństwa, red. *G. Szpor*, *A. Gryszczyńska*, Warszawa 2017; Informacja przestrzenna, red. *G. Szpor*, *K. Czaplicki*, Warszawa 2018; Przetwarzanie danych osobowych, red. *G. Szpor*, *K. Czaplicki*, Warszawa 2019; Analityka danych, red. *G. Szpor*, *K. Czaplicki*, Warszawa 2019; Cyberpandemia, red. *A. Gryszczyńska*, *G. Szpor*, Warszawa 2020; Globalne gry, red. *A. Gryszczyńska*, *G. Szpor*, *W.R. Wiewiórowski*, Warszawa 2022.

Tematem badań w roku 2023 jest solidarność cyfrowa.

Warszawa, kwiecień 2023 r.

Agnieszka Gryszczyńska i *Grażyna Szpor*