INSTYTUT JAGIELLOŃSKI

ZAGROŻENIA WYNIKAJĄCE Z CYBERPRZESTĘPCZOŚCI I WOJNY HYBRYDOWEJ

SZYMON WIECZOREK
MARCIN ROSZKOWSKI

2021

ZAGROŻENIA WYNIKAJĄCE Z CYBERPRZESTĘPCZOŚCI I WOJNY HYBRYDOWEJ

SZYMON WIECZOREK
MARCIN ROSZKOWSKI

Warszawa, listopad 2021

INSTYTUT JAGIELLOŃSKI

Instytut Jagielloński
ul. Marszałkowska 84/92 lok. 115
00-514 Warszawa

jagiellonski.pl
instytut@jagiellonski.pl

PROJEKT I PRODUKCJA:
PIOTR PERZYNA

NOWE**MEDIA24**.PL

ZAGROŻENIA WYNIKAJĄCE Z CYBERPRZESTĘPCZOŚCI I WOJNY HYBRYDOWEJ

SZYMON WIECZOREK
MARCIN ROSZKOWSKI

WARSZAWA, LISTOPAD 2021

INSTYTUT JAGIELLOŃSKI

Spis treści


240

Wstęp

Cyberprzestępczość stanowi znaczącą część współczesnej przestępczości. Dynamiczny wzrostu liczby użytkowników Internetu, rozwój technologii informacyjnych oraz polityczne i gospodarcze procesy globalizacji doprowadziły do przeniesienia się znaczących części codziennego życia, interakcji społecznych, gospodarczych i politycznych do przestrzeni internetowej. Wraz z tymi przemianami doszło również do przeniesienia się przestępczości zorganizowanej do tych samych części cyberprzestrzeni. Z czasem cyberprzestępstwa stały się częstsze, bardziej profesjonalne, a dodatkowo pojawiły się nowe rodzaje czynów zabronionych. Doszło również do zmiany na poziomie strategicznym - coraz rzadziej atakującymi są pojedyncze osoby, a w ich miejsce wchodzą wyspecjalizowane grupy, nierzadko otrzymujące wsparcie od niektórych państw. Rolą niniejszego raportu jest zwrócenie uwagi na skalę zjawiska, przywołanie rodzajów cyberprzestępczości, przywołanie kluczowych historycznych przykładów cyberprzestępstw oraz przybliżenie dostępnych narzędzi i strategii zabezpieczeń.

1. Cyberprzestępczość i cyberbezpieczeństwo

Pojęcie cyberprzestępczości brzmi może brzmieć intuicyjnie, warto jednak przytoczyć jedną z oficjalnych definicji. Komisja Europejska[1] definiuje cyberprzestępstwa jako szeroki wachlarz działalności przestępczej, w ramach której komputery oraz systemy informatyczne są narzędziem przestępczym oraz celem działania przestępczego. W ramach tej definicji, cyberprzestępczość obejmuje zarówno tradycyjne przestępstwa przeniesione do cyberprzestrzeni, jak również nowe rodzaje przestępczości, które pojawiły się wraz z rozwojem technologii informacyjnych.

O skali cyberprzestępczości może świadczyć fakt, że zarówno podmioty prywatne, jak i państwowe są zainteresowane zabezpieczaniem się przed tym zjawiskiem. Ośrodek badawczy cyberprzestępczości, Cybersecurity Ventures[2], szacuje koszty generowane przez to zjawisko dla światowej gospodarki w 2021 na 6 bilionów dolarów amerykańskich, czyli 190 tysięcy dolarów amerykańskich na sekundę. Gdyby potraktować cyberprzestępczość jako osobny kraj, a generowane koszty jako PKB, to opisywane zjawisko byłoby trzecią co do wielkości gospodarką świata po Stanach Zjednoczonych i Chinach.

Cyberprzestępczość wykazuje dynamiczny wzrost swojego znaczenia. Z szacunków wspomnianego wcześniej ośrodka badawczego wynika, że w 2015 ogólnoświatowy koszt cyberprzestępczości wyniósł 3 biliony dolarów amerykańskich. Z kolei prognoza na rok 2025 wskazuje na straty dla globalnej gospodarki rzędu 10.5 biliona dolarów amerykańskich. Taka kwota sugerowałaby wzrost kosztów o 15% w skali roku w latach 2021-25. Zestawienie skali wzrostu zjawiska z prognozą PKB opublikowaną w czerwcu br. przez Bank Światowy[3] prowadzi do ważnego wniosku. Znaczenie cyberprzestępczości jako problemu cywilizacyjnego będzie rosło i w odpowiedzi na to zagrożenie należy zwiększyć wysiłki w ramach walki z tym zjawiskiem.

Także w skali pojedynczych przedsiębiorstw problem cyberprzestępczości prezentuje się niepokojąco. Według raportu Global Crisis Survey[4] autorstwa PwC z 2019 r., 67% przebadanych polskich firm doświadczyło kryzysu w ciągu ostatnich 5 lat. Spośród dostępnych czynników kryzysowych, 22% firm wskazywało na czynniki technologiczne, takie jak awarie technologiczne czy cyberprzestępczość. Na podstawie prognoz wzrostu kosztów generowanych globalnie przez cyberprzestępstwa oraz przenoszenia się kolejnych elementów codziennego życia do świata wirtualnego można przewidywać, że znaczenie tego zjawiska w ramach zarządzania kryzysem będzie rosło.

Odpowiedzią na zagrożenia związane z cyberprzestępczością jest bezpieczeństwo cybernetyczne[5]. Według definicji Komisji Europejskiej z przywołanego wyżej dokumentu, cyberbezpieczeństwo to zbiór zabezpieczeń i działań do wykorzystania w ramach ochrony przestrzeni cybernetycznej, jej dostępności, poufności oraz integralności przed zagrożeniami, na które jest narażona. Przeniesienie znaczących części życia społecznego, kulturalnego, gospodarczego i politycznego do świata wirtualnego powoduje konieczność jego ochrony. Ponieważ cyberprzestrzeń jest większości posiadana i wykorzystywana przez

1 Komisja Europejska, Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

2 Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025" - https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

3 Bank Światowy prognozuje wzrost globalnego PKB w 2022 r. i 2023 r. na odpowiednio 4,3% i 3,1%; Bank Światowy, raport Global Economic Prospects - https://openknowledge.worldbank.org/bitstream/handle/10986/35647/9781464816659.pdf

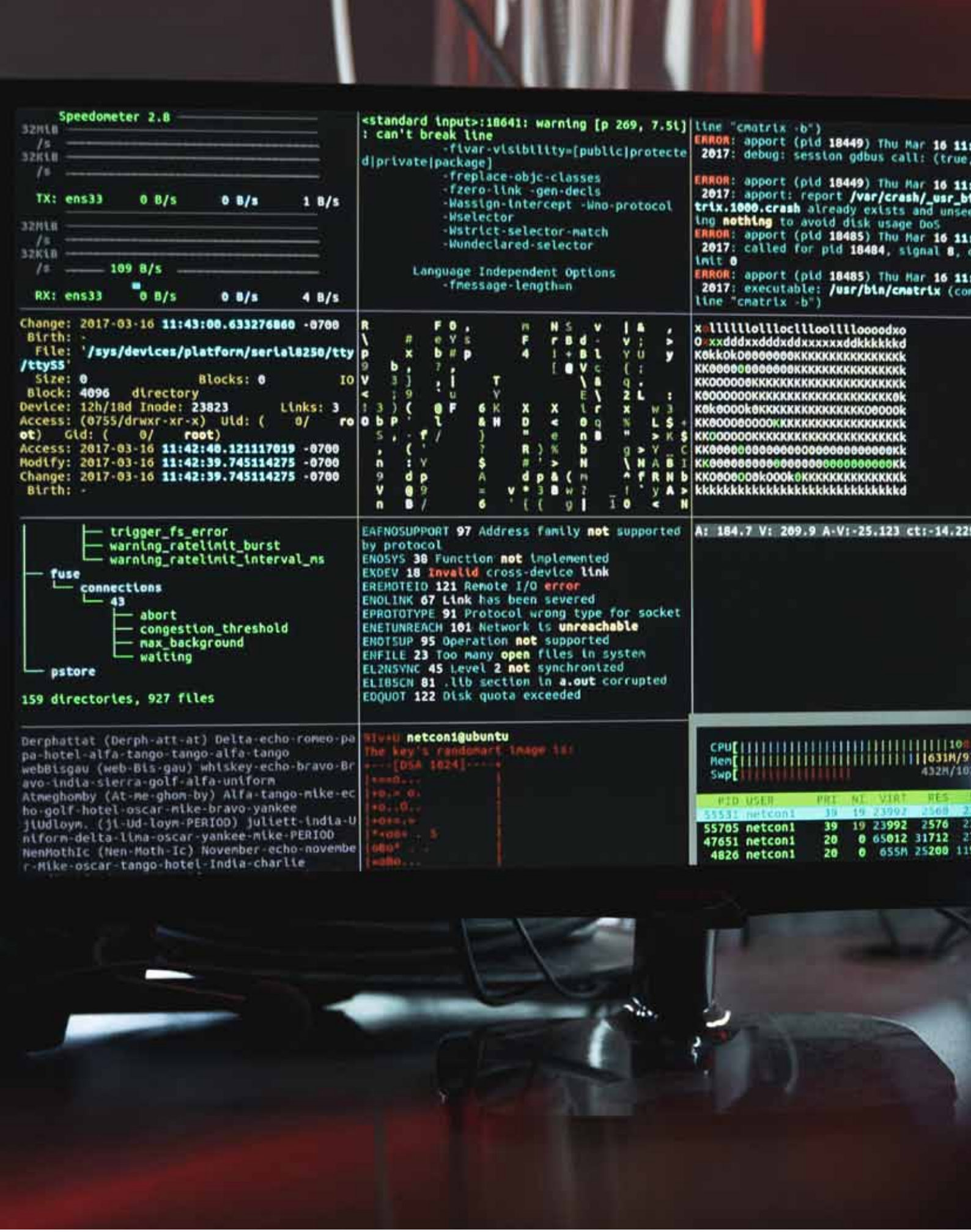
4 PwC – Global Crisis Survey 2019 - https://www.pwc.pl/pl/pdf-nf/2019/global-crisis-survey-2019.pdf

5 Na użytek tego raportu autor używa pojęć „cyberbezpieczeństwo" i „bezpieczeństwo cybernetyczne jako równoważne.

sektor prywatny, zapewnienie jej bezpieczeństwa zależy od skutecznej współpracy sektora publicznego z sektorem prywatnym.

O wadze cyberprzestępczości jako zagadnienia kryminalnego może również świadczyć fakt, iż zarówno podmioty prywatne, jak i państwowe są zainteresowane zabezpieczaniem się przed tym zjawiskiem. Sektor prywatny tworzy i rozwija specjalistyczne oprogramowanie zabezpieczające urządzenia i sieci przed określonymi rodzajami cyberprzestępstw. Organizacja Grand View Research[6] szacuje wartość rynku cyberbezpieczeństwa w 2020 r. na 167 miliardów dolarów amerykańskich, a jego roczny wzrost do 2028 r. na 11 procent. Z kolei sektor państwowy podejmuje się zadania przeciwdziałania oraz ścigania cyberprzestępczości. W tym celu powoływane są specjalistyczne komórki na poziomie poszczególnych krajów, w ramach organizacji międzynarodowych, takich jak np. Unia Europejska czy Organizacja Paktu Północnoatlantyckiego (NATO).

6 Grand View Research, Cyber Security Market Analysis - https://www.grandviewresearch.com/industry-analysis/cyber-security-market


Speedometer 2.8
TX: ens33 0 B/s 0 B/s 1 B/s
RX: ens33 0 B/s 0 B/s 4 B/s
109 B/s
-fvar-visibility=[public|protected|private|package]
-freplace-objc-classes
-fzero-link -gen-decls
-Wassign-intercept -Wno-protocol
-Wselector
-Wstrict-selector-match
-Wundeclared-selector
Language Independent Options
-fmessage-length=n
Change: 2017-03-16 11:43:00.633276860 -0700
Birth: -
File: '/sys/devices/platform/serial8250/tty/ttyS5'
Size: 0 Blocks: 0 IO
Block: 4096 directory
Device: 12h/18d Inode: 23823 Links: 3
Access: (0755/drwxr-xr-x) Uid: (0/ root)
Gid: (0/ root)
Access: 2017-03-16 11:42:40.121117019 -0700
Modify: 2017-03-16 11:42:39.745114275 -0700
Change: 2017-03-16 11:42:39.745114275 -0700
Birth: -
trigger_fs_error
warning_ratelimit_burst
warning_ratelimit_interval_ms
fuse
connections
43
abort
congestion_threshold
max_background
waiting
pstore
159 directories, 927 files
EAFNOSUPPORT 97 Address family not supported by protocol
ENOSYS 38 Function not implemented
EXDEV 18 Invalid cross-device link
EREMOTEIO 121 Remote I/O error
ENOLINK 67 Link has been severed
EPROTOTYPE 91 Protocol wrong type for socket
ENETUNREACH 101 Network is unreachable
ENOTSUP 95 Operation not supported
ENFILE 23 Too many open files in system
EL2NSYNC 45 Level 2 not synchronized
ELIBSCN 81 .lib section in a.out corrupted
EDQUOT 122 Disk quota exceeded
A: 184.7 V: 209.9 A-V:-25.123 ct:-14.22
Derphattat (Derph-att-at) Delta-echo-romeo-papa-hotel-alfa-tango-tango-alfa-tango
webBisgau (web-Bis-gau) whiskey-echo-bravo-Bravo-india-sierra-golf-alfa-uniform
Atmeghomby (At-me-ghom-by) Alfa-tango-mike-echo-golf-hotel-oscar-mike-bravo-yankee
jlUdloym. (jl-Ud-loym-PERIOD) juliett-india-Uniform-delta-lima-oscar-yankee-mike-PERIOD
NenMothIc (Nen-Moth-Ic) November-echo-novembe
r-Mike-oscar-tango-hotel-India-charlie
netcon1@ubuntu
The key's randomart image is:
[DSA 1024]
CPU
Mem
Swp
631M/9
432M/10
PID USER PRI NI VIRT RES
55705 netcon1 39 19 23992 2576
47651 netcon1 20 0 65012 31712
4826 netcon1 20 0 655M 25200

2. Cyfrowy wyścig zbrojeń

Cyberprzestępczość i cyberbezpieczeństwo wykazują duże podobieństwo do wyścigu zbrojeń – oba zjawiska podlegają ciągłemu procesowi ewolucji i konkurują ze sobą. Pojawiają się nowe narzędzia przestępstw, a już istniejące podlegają zmianom w celu zwiększenia ich skuteczności. W tym samym czasie rozwojowi podlegają również praktyki, działania i narzędzia związane z zapewnieniem bezpieczeństwa cyberprzestrzeni. Regularnie dochodziło do przełomów po obu stronach frontu, o czym może świadczyć wycinek historii obu tych zjawisk[7].

Za początki współcześnie rozumianej cyberprzestępczości można uznać lata 80. poprzedniego stulecia[8]. W 1983 r. w użyciu pojawiły się dwa terminy związane ze złośliwym oprogramowaniem – wirus komputerowy oraz koń trojański. Do połowy lat 90. Wirusy komputerowe nauczyły się mutować swój kod w celu uniknięcia wykrycia przez ówczesne antywirusy. Rozwój poczty elektronicznej przyspieszył rozprzestrzenianie się zagrożeń - w 1999 wirus komputerowy Melissa rozprzestrzeniał się drogą mailową, wywołując straty rzędu 80 milionów dolarów amerykańskich. W 2001 r. pojawiła się nowa technika zarażania komputerów –odwiedzenie uszkodzonej witryny internetowej wystarczało do zainfekowania urządzenia, z którego korzystano. W latach 2000. rozwinięto tzw. *„zero-day attacks"* – ataki, które wykorzystują luki systemowe, o których nie wiedzą twórcy aplikacji. Dekadę później 2010. pojawiły się również ataki oparte o inżynierię społeczną.

Za początek cyberbezpieczeństwa można uznać koniec lat 80. XX wieku. W 1987 r. powstały pierwsze programy skanujące komputery w poszukiwaniu wirusów komputerowych. W 1992 r. pojawił się pierwszy program antywirusów, który oprócz skanowania proponował działania do podjęcia względem zainfekowanych plików. W latach 90. naukowiec z NASA stworzył pierwszą zaporę internetową. Na początku lat 2000. pojawiły się darmowe programy antywirusowe. W 2007 r. programy antywirusowe rozbudowano o możliwość badania innych zagrożeń, a rok później wbudowano wyszukiwanie złośliwego oprogramowania. Wraz z rozszerzaniem się dostępu do Internetu oraz smartfonów doszło do rozprzestrzenienia się zabezpieczeń na kolejnych urządzeniach i ich rozwoju. W latach 2010. Rozwinięto kolejne narzędzia cyberbezpieczeństwa, takie jak uwierzytelnianie wielopoziomowe, VPN, zabezpieczenia wbudowane w systemy operacyjne oraz rozbudowano dotychczasowe narzędzia analizy złośliwych plików.

Powyższy rys historyczny świadczy o dynamicznej ewolucji narzędzi cyberprzestępczości oraz bezpieczeństwa cybernetycznego. Zarówno przestępcy, jak i specjaliści od cyberbezpieczeństwa pracują nad poprawą jakości wykorzystywanych przez siebie narzędzi. W przypadku pierwszej grupy jakość oznacza więcej wygenerowanych kosztów oraz więcej pieniędzy uzyskanych z tytułu podejmowanych działań. Z kolei specjaliści od cyberbezpieczeństwa poprzez większą skuteczność swoich produktów dążą do ochrony interesów gospodarczych i wizerunkowych swoich klientów.

7 Fragment na podstawie artykułu o historii cyberbezpieczeństwa, który pojawił się na blogu czeskiego programu antywirusowego Avast - https://blog.avast.com/history-of-cybersecurity-avast

8 Disclaimer – cyberprzestępczość jako taka pochodzi z wcześniejszego czasu niż lata 80. XX w., natomiast dzisiaj nikt w taki sposób nie popełnia przestępstw cybernetycznych.

3. Arsenał cyberprzestępczości

Działania przestępcze w przestrzeni wirtualnej są dokonywane przy użyciu cyberataków. Ich celem jest uzyskanie dostępu do danych, funkcji lub innych zastrzeżonych elementów, do których atakujący nie ma dostępu. Gdy atakującym uda się osiągnąć swoje zamiary, wykorzystują sytuację do odniesienia własnej korzyści, co praktycznie w każdym przypadku oznacza wygenerowanie strat po stronie ofiary.

Cyberataki można zgrupować w następujące cyberprzestępstwa:

1. Kradzież wrażliwych informacji przy użyciu technologii informacyjnych – przeniesienie kradzieży do cyberprzestrzeni. Przestępcy wykradają wartościowe informacje, takie jak informacje niejawne9, własność intelektualna, tajemnice przedsiębiorstwa, korespondencja emailowa, czy dane wrażliwe pracowników. Następnie wymienione informacje są wykorzystywane do różnych celów10, bezpośrednio przez atakujących lub po uprzednim sprzedaniu ukradzionych informacji.

2. Cyberterroryzm – działania przestępcze przy użyciu technologii informacyjnych, mające na celu wymuszenie określonych ustępstw na społeczeństwie i władzach państwowych.

3. Wymuszenia internetowe – działania przestępcze polegające na poddawaniu cyberatakom lub groźbie cyberataków danych witryn internetowych, a następnie proponowaniu zaprzestania takich ataków w zamian za określoną sumę pieniędzy. Wymuszający mogą grozić także wykasowaniem danych lub złamaniem systemów zabezpieczeń danej firmy.

4. Szpiegostwo gospodarcze – Działania szpiegowskie podejmowane w celach uzyskania przewagi gospodarczej nad innym podmiotem. Może być dokonywane zarówno przez firmy prywatne, jak i przez poszczególne państwa.

5. Wojna cybernetyczna – Działania polegające na prowadzeniu ataków na systemy informatyczne wroga przy użyciu komputerów, Internetu, oprogramowania oraz innych narzędzi. W odróżnieniu od wcześniej wymienionych typów przestępstw cybernetycznych, to pojęcie odnosi się dużo większym stopniu do ataków przeprowadzonych ze wsparciem ze strony wyspecjalizowanych komórek współpracujących ze służbami specjalnymi różnych krajów.

Jednym z ważnych powodów, dla których cyberprzestępczość jest relatywnie trudna do zwalczania, jest szeroki zakres dostępnych narzędzi. W zależności od motywów, celów oraz jakości zabezpieczeń, przestępcy mogą wybrać sposób, za pomocą którego chcieliby uzyskać zamierzony efekt.

Istotnym narzędziem cyberataków jest tzw. złośliwe oprogramowanie (ang. malware). Tym mianem określa się ogół programów wykorzystywanych do szkodzenia systemowi komputerowemu oraz jego użytkownikom. Do tego grona zalicza się:

a. Oprogramowanie szantażujące (ang. *ransomware)* – oprogramowanie blokujące dostęp do systemu komputerowego lub uniemożliwiające odczyt zapisanych w nim plików. Co do zasady ten

9 Informacje niejawne zostały zdefiniowane w ramach ustawy Sejmu RP o ochronie informacji niejawnych z 5 sierpnia 2010 r. - https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20101821228/T/D20101228L.pdf

10 Wśród wspomnianych sposobówh można wymienić m.in. zdobywanie nieuczciwej przewagi rynkowej, insider trading, szantaż czy pogorszenie reputacji atakowanej firmy przy użyciu mediów.

rodzaj programów jest wykorzystywany przez przestępców do wymuszania okupu w zamian za przywrócenie stanu początkowego.

b. Oprogramowanie szpiegujące (ang. *spyware*) – programy komputerowe gromadzące informacje o użytkownikach lub organizacjach i przesyłające je innym podmiotom bez wiedzy ofiar.

c. *Scareware* – oprogramowanie wykorzystujące narzędzia inżynierii społecznej w celu wywołania paniki przed rzekomym zagrożeniem. Celem takiej manipulacji jest nakłonienie użytkowników do zakupu niepotrzebnego oprogramowania.

d. *Keylogger* – programy komputerowe lub urządzenia zapisujące klawisze naciskane przez użytkownika. W kontekście cyberprzestępczości keyloggery służą przede wszystkim do zbierania haseł i uzyskiwania dostępu do danych poufnych.

e. Konie trojańskie (ang. *trojan*) – oprogramowanie, które pod przykrywką przydatnej dla użytkownika aplikacji implementuje niepożądane dodatkowe funkcje, takie jak np. wirusy komputerowe.

f. Wirusy komputerowe – programy komputerowe, które mogą powielać się wielokrotnie na urządzeniach. Do swojego działania wykorzystują programy komputerowe, do których dopisują swój kod pozwalający na ich replikację. W efekcie operacje komputerowe stają się wolniejsze, może dojść do zepsucia określonych plików z danymi, wycieku informacji czy uszkodzenia systemu operacyjnego.

Innym kluczowym narzędziem cyberataków są ataki blokujące dostęp potencjalnym użytkownikom witryn internetowych. Atak typu blokada usług (ang. *Denial of Service*, w skrócie DoS) to typ cyberataku, w którym atakujący chce odciąć dostęp użytkownikom do danego systemu komputerowego lub sieci poprzez przeciążenie aplikacji obsługujących system komputerowy lub sieć. Osobną podkategorią ataku typu DoS jest rozproszona blokada usług (ang. *Distributed Denial of Service*, w skrócie DDoS), w której atak na system komputerowy lub sieć jest przeprowadzony z wielu urządzeń, przez co taki atak jest trudniejszy do zablokowania. Obecnie ataki blokujące są coraz rzadsze – witryny internetowe są lepiej zabezpieczone przed nimi, zaś organy ścigania dysponują lepszymi narzędziami wymierzonymi w cyberprzestępców posługujących się atakami DDoS[11].

We współczesnej cyberprzestrzeni istotnym zagrożeniem są również cyberataki typu *phishing*. Przestępcy wykorzystują inżynierię społeczną, podszywając się pod osobę lub instytucję w celu zdobycia jej zaufania. Następnie, oszuści próbują wykorzystać zdobyte zaufanie atakowanej osoby w celu nakłonienia jej do podania swoich danych wrażliwych lub instalacji złośliwego oprogramowania. Ten rodzaj cyberataku jest wykorzystywany do wyłudzania pieniędzy od nieświadomych ofiar.

Szczególne niebezpieczeństwo związane z phishingiem wynika z faktu, iż tego rodzaju ataki są w stanie obejść wiele rodzajów zabezpieczeń. W przypadku tego rodzaju ataków zabezpieczanie się wymaga również odpowiedniego przeszkolenia użytkowników cyberprzestrzeni. Jest to również atak podlegający częstej ewolucji, a jego sprawcy potrafią dostosować swoją manipulację do obecnych trendów i nośnych medialnie tematów.

11 Kaspersky, What is a DDoS attack? - https://usa.kaspersky.com/resource-center/threats/ddos-attacks

4. Cyberprzestępczość w organizacjach - przykłady:

W poprzedniej dekadzie doszło do wielu cyberataków, które były kosztowne dla światowej gospodarki i utrwaliły się w świadomości społecznej. Poniższe przykłady stanowią punkt odniesienia do dyskusji nad cyberbezpieczeństwem. Jednocześnie należy je traktować jako ostrzeżenie przed niedoszacowaniem zagrożenia wynikającego z ataków na przestrzeń wirtualną i ich ciągłej ewolucji. Wiele organizacji poniosło straty materialne i wizerunkowe na skutek nieadekwatnego potraktowania problemu przestępczości w cyberprzestrzeni.

Oprócz zagrożenia dla życia społecznego i gospodarczego, cyberataki powinny być traktowane jako zagrożenie wojskowe. Taki charakter miał atak na cyberprzestrzeń Estonii w 2007 r[12]. Konflikt polityczny między władzą a liczną mniejszością rosyjską o przeniesienie radzieckich cmentarzy wojskowych z ruchliwej części centrum Tallinna przerodził się w konflikt cybernetyczny. 27 kwietnia tego roku doszło do paraliżu stron internetowych estońskich organizacji: parlamentu, ministerstw, banków, gazet, mediów. Akty cyberagresji przeprowadzono z terytorium Federacji Rosyjskiej, przede wszystkim przy użyciu metod DoS i DDoS. Paraliż trwał do 18 maja. Na skutek tych wydarzeń, armie zwiększyły swoje zainteresowanie działaniami w cyberprzestrzeni. Dowodem na to może być założenie przez Organizację Paktu Północnoatlantyckiego rok później centrum cyberbezpieczeństwa sojuszu z siedzibą w estońskiej stolicy.

Żaden podmiot gospodarczy nie jest wolny od cyberprzestępczości, szczególnie firmy międzynarodowe. W kwietniu 2011 r. przeprowadzono cyberatak na japońską korporację Sony[13], w ramach którego przestępcy wykradli dane dot. około 77 milionów użytkowników usług internetowych związanych z konsolą PlayStation oraz około 25 milionów użytkowników związanych z usługą Sony Online Entertainment. Atak sparaliżował niektóre z oferowanych usług. Ponadto atakujący uzyskali dostęp do ok. 12 tysięcy kart kredytowych w zaszyfrowanej formie. Zdaniem Sony żaden użytkownik usług sieciowych PlayStation nie został okradziony. Tym niemniej korporacja poniosła straty wizerunkowe oraz w wyniku paraliżu, które zostały wycenione na 171 milionów dolarów amerykańskich.

W sierpniu 2013 r. doszło do cyberataku na globalną wyszukiwarkę Yahoo[14]. W jego wyniku wykradziono dane dot. 3 miliardów użytkowników, wliczając w to multikonta. Wykradzione dane dotyczyły podstawowych informacji kontaktowych z użytkownikami jednak hasła, informacje o kontach bankowych i kartach kredytowych nie zostały wykradzione. Dane te były chronione przez przestarzałe szyfrowanie, system zawierał niezaszyfrowane pytania bezpieczeństwa oraz zastępcze adresy mailowe. Kolejna kradzież danych przydarzyła się rok później na nieznacznie mniejszą skalę. Na skutek tych wydarzeń Yahoo zostało zakupione przez konglomerat telekomunikacyjny Verizon za kwotę mniejszą o 350 milionów dolarów od początkowej oferty.

W 2017 roku został przeprowadzony cyberatak o zasięgu światowym. 12 maja ransomware WannaCry[15], zaatakował ok. 300 tysięcy systemów należących do ok. 30 tysięcy organizacji ze 150 krajów. Za odblokowanie zaszyfrowanych plików oprogramowanie żądało od 300 do 600 dolarów amerykańskich w kryptowalucie bitcoin. Ransomware wykorzystywał lukę w systemie Windows, która została uprzednio uzupełniona w ramach aktualizacji systemu operacyjnego. Na atak były narażone te komputery, które

12 CCDCOE, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective - https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

13 BBC News, Sony faces legal action over attack on PlayStation network - https://www.bbc.com/news/technology-13192359

14 Reuters, Yahoo says all three bilion accounts hacked in 2013 data theft - https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1

15 Atlas Magazine, WannaCry: a ransomware cyber-attack of unprecedented scale - https://www.atlas-mag.net/en/article/wannacry-a-ransomware-cyber-attack-of-unprecedented-scale

nie przeprowadziły stosownych aktualizacji. Wśród poszkodowanych były m.in.: system ochrony zdrowia Wielkiej Brytanii (NHS), ministerstwo spraw wewnętrznych Federacji Rosyjskiej, hiszpański operator telefoniczny Telefónica, niemiecki państwowy operator kolei Deutsche Bahn czy japoński producent samochodów Nissan. Polska nie została dotknięta przez atak tego wirusa. Stany Zjednoczone i Wielka Brytania oskarżają Koreę Północną o przeprowadzenie tego ataku.

W tym samym roku przeprowadzono podobny atak, lecz w tym przypadku celem był jeden kraj. 27 lipca doszło do serii cyberataków na ukraińskie instytucje[16], takie jak banki, ministerstwa, gazety, kijowskie metro i firmy energetyczne. W podobny sposób do WannaCry, złośliwe oprogramowanie wykorzystywało tę samą lukę w systemie Windows, która została już uzupełniona. Pomimo tego, że cyberprzestrzeń Ukrainy została zaatakowania przy użyciu ransomware, eksperci sugerują dążenie atakujących do sparaliżowania kraju zamiast uzyskania jak największej ilości pieniędzy z tytułu okupu. Świadczy o tym kilka cech tego ataku. Po pierwsze, został on przeprowadzony w przededniu ukraińskiego święta państwowego, jakim jest Dzień Konstytucji. Po drugie, wiele plików pod kontrolą złośliwego programu zostało permanentnie uszkodzone. Po trzecie, istnieją podejrzenia, że ataku dokonano z terytorium Federacji Rosyjskiej. Warto wspomnieć, że do podobnych ataków, aczkolwiek na mniejszą skalę, dochodziło także m.in. na terenie Francji, Niemiec, Polski, Wielkiej Brytanii czy Stanów Zjednoczonych.

Do ataków ransomware dochodzi również na pojedyncze organizacje. Taki atak przeprowadzono 14 maja 2021 na system ochrony zdrowia Irlandii[17] (*Health Service Executive*, w skrócie HSE) przy użyciu ransomware. Atak sparaliżował system informatyczny organizacji. W jego wyniku odwołano wiele wizyt lekarskich, szpitale dotknięte atakiem wróciły do papierowego systemu rejestracji, a testy na COVID-19 musiały być przeprowadzane z pominięciem rezerwacji. Ponadto w wyniku ataku doszło do wycieku poufnych danych medycznych oraz korespondencji internetowej dotyczących 520 pacjentów. Jako sprawców ataku zidentyfikowano grupę cyberprzestępczą działającą z terytorium Federacji Rosyjskiej. Dużym faktorem w tym paraliżu była ówczesna sytuacja w irlandzkim Narodowym Centrum Cyberbezpieczeństwa (NCSC), które wówczas zatrudniało 25 osób, jego roczny budżet wynosił 5 milionów euro, a stanowisko prezesa było nieobsadzone od roku, z powodu nieadekwatnego wynagrodzenia w stosunku do wymaganych kompetencji i ponoszonej odpowiedzialności.

Z zagrożeniami cyberbezpieczeństwa można spotkać się także w polskiej cyberprzestrzeni. Od co najmniej kilku miesięcy w polskim Internecie funkcjonuje oszustwo phishingowe. Podszywając się pod rozpoznawalny portal internetowy, powołując się na rzekomą sensację związaną z danym artystą, sportowcem, politykiem lub dziennikarzem, autorzy oszustwa przekierowują na starannie przygotowaną przez siebie treść. Na sfabrykowanych stronach znajdują się spreparowane treści reklamujące pozornie lukratywną inwestycję. Jest ona firmowana autorytetem znanej osoby, fałszywymi komentarzami osób zadowolonych, a często także przygotowanych materiałów wideo. Dodatkową warstwę presji tworzy informacja o ograniczonej liczbie osób mogących skorzystać z tej oferty.

Postępując według scenariusza sugerowanego przez wyłudzaczy, osoba zostawia informacje kontaktowe. Gdy do tego dojdzie, w ciągu najbliższych kilkunastu godzin dzwoni do niej odpowiednio przeszkolony rozmówca reprezentujący oszustów. Roztaczając wizję zysków, prosi o wpłatę środków na inwestycję. W kolejnych rozmowach osoba kontaktowa przekonuje ofiarę o dotychczas wypracowanych dużych zyskach z jej wpłaty i sugeruje dalsze przelewy na poczet inwestycji. Sytuacja trwa do czasu, gdy ofiara decyduje się na wypłatę „zarobionych" pieniędzy. Wówczas przestępcy zasłaniają się potrzebnymi ubez-

16 Reuters, Ukrainian banks, electricity firm hit by fresh cyber attack - https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ

17 Reuters, Irish health service hit by 'very sophisticated' ransomware attack - https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

pieczeniami, gwarancjami oraz zgodami. Oszuści nigdy nie planują zwrotu wpłaconych środków i zrobią wszystko, żeby do tego nie doszło.

Istnieją cechy charakterystyczne oszustw typu *phishing*, na podstawie których można je zidentyfikować. Po pierwsze, tego rodzaju oszustwa sugerują dokonanie inwestycji o znacznie wyższych stopach zwrotu niż te oferowane przez banki czy fundusze inwestycyjne. Po drugie, przestępcy powołują się na autorytet rozpoznawalnej osoby lub organizacji. Po trzecie, przypadki phishingu funkcjonujące w polskiej cyberprzestrzeni powstają na terenie byłych republik Związku Radzieckiego. W związku z tym ich autorzy popełniają błędy gramatyczne, interpunkcyjne i literowe typowe dla użytkowników języków wschodniosłowiańskich. Te błędy wynikają w dużej mierze z zapisywania oryginalnych komunikatów przy użyciu cyrylicy. Po czwarte, oszuści tworzą presję na skorzystanie z proponowanej przez siebie oferty możliwie jak najszybciej. Do tego celu wykorzystują efekt psychologiczny zwany strachem przed pominięciem (ang. *Fear of missing out*, w skrócie FOMO), wykorzystując niepokój i strach ofiary przed utratą szansy na poprawienie swojej sytuacji. Po piąte, podmioty oferujące podejrzane inwestycje znajdują się często na liście ostrzeżeń publicznych Komisji Nadzoru Finansowego.

5. Jak zabezpieczać się przed cyberprzestępczością?

Cyberataki mogą powodować znaczące straty finansowe oraz wizerunkowe. Z tego powodu organizacje podejmują wysiłki w celu zarządzania ryzykiem bycia ofiarą cyberprzestępstwa. W tym celu wypracowują procedury cyberbezpieczeństwa oraz wykorzystują odpowiednie zabezpieczenia w celu minimalizacji potencjalnych kosztów.

Do grona zabezpieczenień przed cyberatakami w formie oprogramowania należą:

1. Zapora sieciowa (ang. *firewall*) – system bezpieczeństwa sieciowego, który monitoruje i kontroluje przepływ pakietów połączeń sieci internetowej w oparciu o zdefiniowane zasady bezpieczeństwa.

2. Oprogramowanie antywirusowe – Programy komputerowe wykorzystywane do zapobiegania, wykrywania i usuwania złośliwego oprogramowania. Współczesne programy antywirusowe mogą również chronić przed innymi zagrożeniami, takimi jak zainfekowane strony internetowe czy ataki DDoS.

3. Wirtualna sieć prywatna (VPN) – usługa pozwalająca na łączenie się z Internetem poprzez wirtualny, zaszyfrowany tunel. Wykorzystując taką sieć, do standardowego kontaktu pomiędzy dostawcą i odbiorcą pakietów danych internetowych dochodzi podmiot pośredniczący – serwer, przez który przechodzi dane połączenie. Podstawowymi zaletami wykorzystywania VPN są prywatność oraz trudność złamania szyfru dla atakujących cyberprzestępców.

4. Weryfikacja wieloetapowa – sposób zabezpieczenia dostępu do zasobów cyfrowych, w którym użytkownik dostaje dostęp dopiero po udowodnieniu określoną liczbę razy w określony sposób, że to właśnie on jest osobą uprawnioną do korzystania z określonego zasobu. Ta forma kontroli wykorzystywana jest m.in. w ramach kont bankowych, skrzynek e-mail, systemów VPN wykorzystywanych przez organizacje.

4. System wykrywania włamań (ang. *Intrusion Detection System*, w skrócie IDS) – urządzenie lub aplikacja monitorująca cyberprzestrzeń w poszukiwaniu podejrzanej aktywności sieciowej. W ramach systemu zagrożenia są raportowane w celu ograniczenia szkód doznanych ze strony atakujących.

6. Oprogramowanie wykorzystujące algorytmy uczenia maszynowego – zbiorcze określenie programów komputerowych, wykorzystujących opisane algorytmy. Wraz ze wzrostem częstotliwości, poziomu zaawansowania cyberataków oraz zmiany ich charakteru tradycyjne zabezpieczenia mogą nie wystarczać. Modele uczenia maszynowego są w stanie dostosowywać się do nowych zagrożeń bez ingerencji użytkownika.

Organizacje decydują się również na wprowadzenie procedur związanych z cyberbezpieczeństwem oraz zarządzaniem ryzykiem informatycznym. Wśród takich działań można wymienić m.in. następujące:

- Identyfikacja kluczowych aktywów firmy, które wymagają szczególnej ochrony przed cyberatakami,
- Wyznaczenie odpowiednich osób, do których informacja o potencjalnym cyberataku powinna trafiać jako pierwsza,
- Poddawanie systemów bezpieczeństwa regularnym audytom, w ramach których sprawdzane są słabe punkty w systemach wykorzystywanych na dany moment,
- Transfer ryzyka poprzez zakup ubezpieczenia pokrywającego szkody wywołane przez cyberataki.

Na osobną uwagę zasługują szkolenia z zakresu cyberbezpieczeństwa. Zabezpieczanie się za pomocą oprogramowania rozwiązuje część problemu – jeżeli cyberatak przejdzie przez zabezpieczenia, wówczas powstaje ryzyko nawiązania kontaktu z urządzeniem wykorzystywanym przez pracownika organizacji. Z kolei procedury związane z cyberbezpieczeństwem nie są wystarczająco skuteczne, jeżeli wszyscy pracownicy organizacji nie są świadomi wymaganych od nich działań i środków ostrożności. Ponadto zagrożenia cyberatakami ulegają zmianom i wiedza o zabezpieczaniu się podlega dezaktualizacji. Z powyższych względów organizacje decydują się na prowadzenie szkoleń dla pracowników, w których uświadamiane są bieżące zagrożenia, sposoby przeciwdziałania oraz minimalizacji potencjalnych kosztów cyberataku.

6. Podsumowanie

Cyberprzestępczość stanowi poważne zagrożenie dla współczesnego życia społecznego, politycznego i gospodarczego. Zjawisko jest w trakcie trendu wzrostowego ze względu na potencjalny dalszy rozwój technologii informacyjnych i komunikacyjnych oraz przenoszenie się kolejnych elementów życia codziennego do przestrzeni wirtualnej. Do tej pory doszło do wielu przypadków cyberataków, które wygenerowały wielomilionowe straty. Wiele z nich zostało zapamiętanych jako ich podręcznikowe przykłady, dające również dowód na to, do czego mogą prowadzić zaniechania w zakresie cyberbezpieczeństwa. Żadna organizacja nie może czuć się wolna od ataków na jej własną część przestrzeni wirtualnej.

Zabezpieczanie się przed cyberatakami jest możliwe i kluczowe do prawidłowego funkcjonowania cyberprzestrzeni. Jest to warunek konieczny nie tylko z punktu widzenia gospodarki i dobrobytu obywateli, ale także z perspektywy bezpieczeństwa narodowego. Oprogramowanie, procedury i podnoszenie świadomości o problemie mogą poprawić bezpieczeństwo i uchronić przed cyberprzestępcami. W ten sposób można ograniczać koszty ponoszone przez gospodarkę oraz wpływy niepożądanych aktorów na życie gospodarcze, społeczne i polityczne zarówno w obrębie poszczególnych krajów, jak również gospodarki światowej.

INSTYTUT JAGIELLOŃSKI

Instytut Jagielloński
ul. Marszałkowska 84/92 lok. 115
00-514 Warszawa

jagiellonski.pl
instytut@jagiellonski.pl

2021