Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/1-12 | strony: 121–130

Romuald Hoffmann
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Systemów Informatycznych
romuald.hoffmann@wat.edu.pl

Ogólny cykl życia ataku cybernetycznego i jego markowowski model

JEL: C02, C6, D81, L86
Słowa kluczowe: atak cybernetyczny, cyberatak, cykl życia ataku cybernetycznego, proces Markowa dyskretny w stanach, łańcuch Markowa z ciągłym parametrem
Streszczenie. W pracy zaproponowano ogólny cykl życia ataku cybernetycznego, który wyróżnia się od publikowanych w literaturze zasadniczo dwiema dodatkowymi fazami: identyfikacji potrzeb atakującego oraz zakończenia ataku cybernetycznego. Na bazie zdefiniowanego cyklu życia ataku przedstawiono stochastyczny model opisujący jego funkcjonowanie. Model bazuje na jednorodnym łańcuchu Markowa z ciągłym czasem.

Wprowadzenie

W historii przestępczości komputerowej było już wiele spektakularnych cyberataków, które opisywano zarówno w prasie, jak i szeroko omawiano w wielu periodykach naukowych. Ogół społeczeństwa dowiedział się tylko o tych najbardziej spektakularnych i/lub wyrafinowanych, i jednocześnie interesujących. Ale statystyki prowadzone przez dostawców systemów antywirusowych pokazują, że sumaryczna liczba ataków w skali sieci globalnej to rząd tysięcy dziennie. To pokazuje, że w dzisiejszych czasach cyberataki to właściwie już codzienność, a najgorsze jest to, że wciąż będzie ich przybywać. Można powiedzieć, że cyberprzestępcy to gangsterzy XXI wieku, przed którymi, na obecnym etapie rozwoju technologicznego, powszechności urządzeń komputerowych, ale i niefrasobliwości użytkowników, bardzo trudno się obronić. Do tej pory wiele państw, firm, organizacji, jak i zwykłych ludzi, boleśnie tego doświadczyło.

W tym świecie atakujący to nie tylko pojedynczy przestępcy czy grupy cyberprzestępców, dla których rzemiosło to stało źródłem dochodów[1], ale również niektóre państwa, dla których ataki w cyberprzestrzeni stały się elementem polityki. Dla wielu państw również Internet[2] stał się areną walki cybernetycznej. Przykłady funkcjonowania programów takich, jak np. Stuxnet, Flame czy Duqu pokazują, że prawdopodobna rywalizacja państw w cyberprzestrzeni stała się faktem. Nie popełnimy błędu, ryzykując stwierdzenie, że problem ten narasta, co może, zdaniem autora, prowadzić w konsekwencji do międzypaństwowego swoistego „wyścigu zbrojeń cybernetycznych". Dzisiaj cybernetyczny atak to już nie kwestia odpowiedzi na pytanie „czy", ale odpowiedzi na pytanie: kiedy i z jakim prawdopodobieństwem. Zatem musimy uświadomić sobie, że atak cybernetyczny na naszą infrastrukturę, w tym usługi elektroniczne, jest tylko kwestią czasu.

Pomimo tego, jak często mówi się i pisze o cyberatakach, nawet jeszcze dzisiaj wiele organizacji i ludzi odbiera atak cybernetyczny jako zdarzenie, któremu praktycznie nie da się przeciwstawić. Jednak w rzeczywistości atak cybernetyczny nie trwa krótką chwilę, ale jest procesem[3], czyli zbiorem czynności, które należy wykonać w odpowiedniej kolejności i które mają swój czas trwania i miejsce. Czynności te łączy się w logiczne grupy i realizuje się etapowo, tworząc w ten sposób proces ataku cybernetycznego, który ma skończony czas trwania i można nazywać go cyklem życia ataku cybernetycznego (*cyber attack life cycle*[4]). Znajomość cyklu ataku może umożliwić np. szacowanie: prawdopodobieństwa ataku, średniego czasu trwania ataku lub średniego czasu do kompromitacji systemu (*time-to--compromise*). Znając te wymienione i inne charakterystyki procesu, możemy próbować odpowiedzieć na postawione przed chwilą pytanie, kiedy i z jakim prawdopodobieństwem. W tym celu musimy najpierw przebadać stochastyczną naturę procesu ataku. Aby to zrobić, w artykule nakreślono ogólny proces ataku cybernetycznego, który nazwano „ogólnym cyklem życia ataku cybernetycznego", składającym się z następujących siedmiu faz: identyfikacja i definicja (potrzeb), rozpoznanie, uzbrojenie, dostarczenie, uruchomienie i kontrola kodu złośliwego, realizacja celów, zakończenie ataku i zatarcie śladów. Następnie na tej bazie zbudowano stochastyczny model cyklu.

---

1 Np. ataki typu *ransomware*.

2 Największa składowa ogólnie pojętej cyberprzestrzeni.

3 Tym samym organizacje mogą wykryć i powstrzymać atak.

4 W środowisku militarnym: *cyber kill chain.*

1. Cykl życia ataku cybernetycznego w literaturze

W literaturze etapy (fazy) procesu cyberataku, ich liczba oraz rola są różnie definiowane i opisywane. Według (US) Air Force Institute of Technology proces ten składa się z pięciu etapów:[5] rozpoznanie (rekonesans), skanowanie, dostęp do systemu, instalacja kodu złośliwego, eksploatacja kodu złośliwego (Coleman, 2012, s. 106–107). Lockheed Martin (Hutchins, Cloppert, Amin, 2011), po przeanalizowaniu ataków APT[6], proces ataku cybernetycznego definiuje jako ciąg siedmiu etapów[7]: rozpoznanie, uzbrojenie, dostarczenie, eksploracja[8], instalacja, kierowanie i dowodzenie, akcja, tzn. atak celu. Proces ten również opisują Spring, Hatleback (2017) oraz Khan, Siddiqui i Ferens (2018). Natomiast Hahn, Thomas, Lozano, Cardenas (2015) wskazują na sześć faz w tzw. ujęciu tradycyjnym[9]: rozpoznanie, uzbrojenie, dostarczenie, eksploracja, kierowanie i dowodzenie, osiągnięcie celu. Jednocześnie Hahn i inni (2015) wskazują, że atak na infrastrukturę krytyczną należy rozpatrywać jako ciąg czterech faz[10] następujących bezpośrednio po sobie: 1) rozpoznanie trzech warstw systemowych: systemów informatycznych, systemów sterowania automatyką, układów urządzeń fizycznych; 2) uzbrojenie; 3) dostarczenie kodu złośliwego; 4) realizacja (obejmująca trzy fazy tradycyjne: eksploracji, kierowania i dowodzenia, osiągnięcia celu) oraz dwóch faz[11] zazębiających się wzajemnie: 5) zakłócenie sterowania automatyką zazębiająca się z czwarta fazą (realizacji) oraz 6) atak na fizyczne urządzenia.

Warto zauważyć, że w zależności od typu ataku, niektóre etapy omawianego procesu mogą zostać pominięte przez agresora (Khan i in., 2018).

W wyżej wymienionych i omówionych podejściach opisujących proces ataku cybernetycznego nie uwzględnia się zarówno fazy inicjującej proces, jaką jest uświadomienie, identyfikacja i określenie potrzeb jak i etapu[12] zaprzestania ataku połączonego z zatarciem śladów. Zatarcie śladów oczywiście jest możliwe jeżeli atak nie jest atakiem destrukcyjnym, w którym np. następuje skasowanie danych, znaczne uszkodzenie sprzętu, destrukcja systemu operacyjnego lub systemu informatycznego.

---

[5] *Reconnaissance, scanning, system access, malicious activity, exploitation.*

[6] *Advanced Persistent Threats*.

[7] *Reconnaissance, weaponization, delivery, exploitation, installation, C2, action*; Lockheed Martin proces ten nazywa *cyber kill chain.*

[8] Np. wykorzystanie podatności oprogramowania.

[9] *Reconnaissance, weaponization, delivery, exploitation, C2, achieve objective.*

[10] *Reconnaissance, weaponization, delivery, cyber execution.*

[11] *Control perturbation, physical objective realization.*

[12] Który może być opcjonalny.

2. Proponowany ogólny cykl życia ataku cybernetycznego

Na potrzeby dalszych rozważań przyjmiemy proces ataku składający się z następujących faz[13]: (S_1) identyfikacja i definicja (potrzeb), (S_2) rozpoznanie (*reconnaissance*), (S_3) uzbrojenie (*weaponization*), (S_4) dostarczenie (*delivery*), (S_5) uruchomienie i kontrola kodu złośliwego (*cyber execution and command* & *control*), (S_6) realizacja celów (*achieve objectives*), (S_7) zakończenie ataku i zatarcie śladów. Tak zdefiniowany proces nazywać będziemy ogólnym cyklem życia ataku cybernetycznego. Uszczegółowiony opis faz proponowanego cyklu życia cyberataku zawarto w tabeli 1. Przedstawiony cykl życia ataku stanowi uogólnienie wcześniej prezentowanych podejść (w części 1 artykułu).

Tabela 1. Fazy ogólnego cyklu życia ataku cybernetycznego

Nazwa fazy (symbol fazy)	**Opis fazy (przykład)**
Identyfikacja i definicja (S_1)	Identyfikacja i określenie potrzeb agresora/atakującego np.: „biznesowych", politycznych itp. Faza ta powinna wystąpić nawet, gdyby był to tylko pomysł przestępcy na przejęcie np. konta ofiary na twitterze. Na pewno występuje wówczas, gdy np. grupa przestępcza lub jakaś organizacja planuje swoje działania, wynika z przyjętej szerszej strategii państwa działań w cyberprzestrzeni itp.
Rozpoznanie (*reconnaissance*) (S_2)	Identyfikacja i dobór celów ataków (technicznych) poprzez rozpoznanie docelowego środowiska, np. skanowanie portów TCP, indeksowanie witryn internetowych, materiałów konferencyjnych, list adresów e-maili, sieci społecznościowych, informacji na temat stosowanych (specyficznych) technologii, socjotechniczne wyłudzenie informacji i danych itp.
Uzbrojenie (*weaponization*) (S_3)	Przygotowanie cyberbroni, tzn. specjalnego oprogramowania, np. zintegrowanie koni trojańskich z innym złośliwym kodem (*exploit*) w celu stworzenia możliwego do dostarczenia ładunku za pomocą automatycznego narzędzia (*weaponizer*). W przypadku, gdy nie zachodzi potrzeba budowy lub skonfigurowania pakietu oprogramowania, etap może zostać pominięty
Dostarczenie (*delivery*) (S_4)	Skopiowanie cyberbroni do docelowego środowiska, np. wykorzystanie najbardziej rozpowszechnionych sposobów dostawy (np. w ramach ataków APT), którymi przykładowo są: zainfekowane załączniki do e-maili, spreparowane lub złośliwie zmodyfikowane oprogramowanie strony internetowej (np. aplety, linki), wstrzyknięcie kodu SQL, zainfekowane nośniki danych podłączane do portów USB

[13] Angielskie nazwy faz wskazują na związek z istniejącymi opisami w literaturze.

Nazwa fazy (symbol fazy)	**Opis fazy (przykład)**
Uruchomienie i kontrola kodu złośliwego (*cyber execution*) (S_5)	Uruchomienie kodu złośliwego (po dostarczeniu cyberbroni do środowiska docelowego), np. w wyniku wykorzystania podatności/luki programowej w aplikacji lub systemie operacyjnym lub zmanipulowania użytkownika systemu docelowego. Instalacja dodatkowego kodu złośliwego, np. koni trojańskich (*Remote Access Trojan* – RAT), umieszczenie tylnych furtek (*backdoor*) w systemie docelowym w celu zestawienia stałego kanału komunikacji zainfekowanego środowiska wewnętrznego ofiary z centrum (zewnętrznym środowiskiem) dowodzenia i sterowania oprogramowaniem złośliwym. Kontrola i sterowanie zainfekowanego środowiska, np. eskalacja lub uzyskanie dodatkowych uprawnień, systemowych, doinstalowanie pozostałego lub dodatkowego kodu złośliwego (np. *backdoor/trojan/rootkit*), modyfikacja system plików, przeglądanie lub modyfikacja systemowych baz danych
Realizacja celów (Achieve Objectives) (S_6)	Podjęcie działań nakierowanych na osiągnięcie pierwotnych celów, np. skopiowanie danych, naruszanie integralności i/lub dostępności danych, uzyskanie dostępu do poczty elektronicznej ofiary w celu wykorzystania jej do głębszej penetracji zakatowanej infrastruktury lub wykorzystanie poczty elektronicznej do dalszego rozprzestrzenienia prowadzonego ataku. W tej fazie nie wyklucza się fizycznej destrukcji infrastruktury organizacji
Zakończenie ataku i zatarcie śladów (S_7)	Zakończenie ataku, może być połączone z usunięciem lub zamaskowaniem śladów ataku i aktywności kodu złośliwego. Etap opcjonalny, zależny od celów i stopnia zaawansowania technologicznego agresora

Źródło: opracowanie własne.

3. Model

Założenia

U podstaw modelu stochastycznego leży zaproponowany ogólny cykl życia ataku cybernetycznego (opis – tab. 1). Przyjmujemy, że nie ma możliwości powrotu (cofnięcia się) do fazy poprzedniej. Natomiast w modelu uwzględnimy dynamikę procesu ataku zakładając, że atak może zostać przeprowadzony z pominięciem fazy uzbrojenia oraz że atak może zostać przerwany w dowolnej chwili.

W pracy przyjmiemy, że wszystkie rozkłady opisujące zachowanie się rozważanego cyklu są rozkładami wykładniczymi o stałych parametrach i wszystkie zmienne losowe opisujące zachowanie się faz cyklu są stochastycznie niezależne. Wobec tego zachowanie się procesu ataku opiszemy za pomocą jednorodnego łańcucha Markowa z czasem ciągłym[14]. Przez kolejne stany procesu rozumiemy odpowiednie fazy cyklu

[14] Jednorodny proces Markowa dyskretny w stanach z ciągłym parametrem czasu.

życia ataku (tab. 1). Dodatkowo wprowadzamy stan procesu odpowiadający sytuacji przerwania ataku[15] z różnych powodów, np. z powodu zmiany zamiaru przez agresora, wykrycia i zablokowania jego działań przez mechanizmy obronne atakowanego systemu itp.

Przyjęte oznaczenia

Na potrzeby dalszych rozważań przyjmujemy następującą konwencję oznaczeń. Niech $X(t)$ będzie procesem stochastycznym (procesem Markowa) zależnym od ciągłego parametru t ($0 \leq t < \infty$) i skończoną liczbą stanów i opisującym zachowanie się cyklu proponowanego cyklu życia ataku. Przez stan S_i przyjmujemy oznaczać stan procesu $X(t)$, gdzie i oraz j oznaczają numery stanów ($i, j = 1, 2,..., 8$). Stany $S_1, S_2,..., S_7$ odpowiadają poszczególnym fazom cyklu (tab. 1). Stan S_8 natomiast odpowiada sytuacji przerwania ataku. Wobec tego zbiór $\{S_1, S_2,..., S_8\} = \{S_i\}_{i=\overline{1,8}}$ jest zbiorem stanów procesu $X(t)$. Przez $p_{ij}(t)$ oraz λ_{ij} oznaczać będziemy odpowiednio: prawdopodobieństwo przejścia w chwili $t \geq 0$ oraz intensywność przejścia[16] procesu $X(t)$ ze stanu S_i do stanu S_j. Zakładamy, że znane są intensywności przejścia. Macierz intensywności przejścia procesu oznaczamy przez Λ ($\Lambda = [\lambda_{ij}]_{8x8}$). Natomiast symbolem $P_i(t)$ przyjmujemy oznaczyć prawdopodobieństwo przebywania procesu $X(t)$ w stanie S_i w chwili $t \geq 0$.

Macierz przejść, układ równań Kołmogorowa, graf Markowa

Wobec przyjętych założeń modelem zachowania się proponowanego w artykule ogólnego cyklu życia ataku cybernetycznego jest jednorodny proces Markowa $X(t)$ z czasem ciągłym $0 \leq t < \infty$ i skończoną liczbą stanów $\{S_i\}_{i=\overline{1,8}}$.

Macierz Λ intensywności przejścia między stanami tego procesu ma postać:

$$\Lambda = \begin{bmatrix} -\lambda_{11} & \lambda_{12} & 0 & 0 & 0 & 0 & 0 & \lambda_{18} \\ 0 & -\lambda_{22} & \lambda_{23} & \lambda_{24} & 0 & 0 & 0 & \lambda_{28} \\ 0 & 0 & -\lambda_{33} & \lambda_{34} & 0 & 0 & 0 & \lambda_{38} \\ 0 & 0 & 0 & -\lambda_{44} & \lambda_{45} & 0 & 0 & \lambda_{48} \\ 0 & 0 & 0 & 0 & -\lambda_{55} & \lambda_{56} & 0 & \lambda_{58} \\ 0 & 0 & 0 & 0 & 0 & -\lambda_{66} & \lambda_{67} & \lambda_{68} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (1)$$

gdzie $\lambda_{ii} = \sum_{\substack{j=1 \\ j \neq i}}^{8} \lambda_{ij}$ oraz $\lambda_{ij} \geq 0$ dla każdego $i, j = 1, 2,..., 8$

[15] Oznaczymy symbolem S_8.

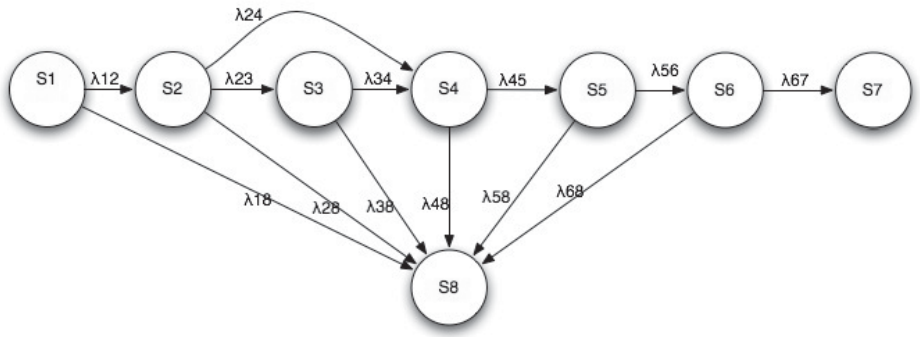
[16] Niezależna od czasu.

Układ równań Kołmogorowa pozwalający na wyznaczenie wektora rozkładu prawdopodobieństw procesu Markowa z macierzą intensywności Λ jest postaci:

$$\left[\frac{d}{\mathrm{dt}}P_0(t) \quad ... \quad \frac{d}{\mathrm{dt}}P_8(t)\right] = [P_0(t) \quad ... \quad P_8(t)] \cdot \Lambda\,,\ t \geq 0 \qquad (2)$$

z warunkiem początkowym $P_1(0) = 1$ oraz $P_i(0) = 0$ dla $i = 2, 3,..., 8$.

Na rysunku 1 przedstawiono graf Markowa obrazujący stany procesu stochastycznego $X(t)$ i intensywności przejścia pomiędzy poszczególnymi stanami.



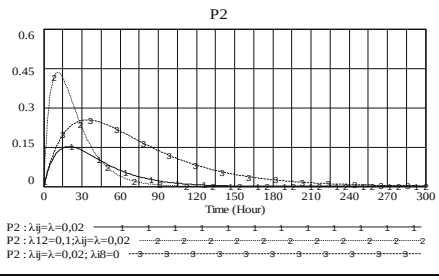
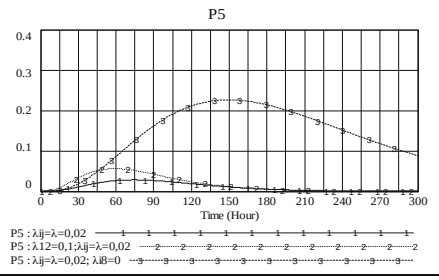
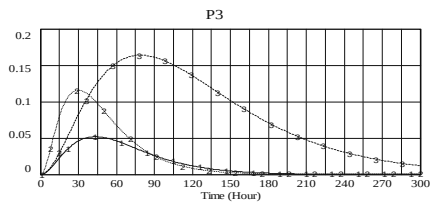
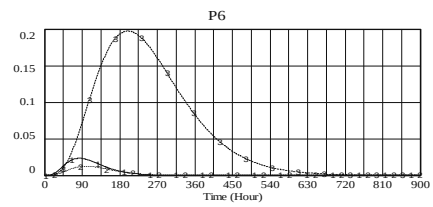
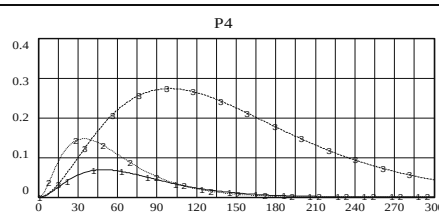
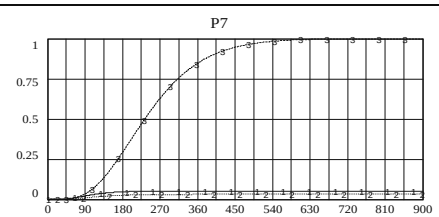
Rysunek 1. Graf Markowa – graf stanów procesu $X(t)$

Źródło: opracowanie własne.

Rozwiązanie numeryczne

Układ równań Kołmogorowa (2) został rozwiązany numerycznie za pomocą pakietu symulacyjnego dynamiki systemowej Vensim® ver. 5 firmy Ventana Systems, Inc. Przykładowe wyniki przeprowadzonych obliczeń zawarto w tabeli 2.

Tabela 2. Przykładowe wyniki numerycznego rozwiązania układu równań Kołmogorowa

Dotyczy faz S_2, S_3, S_4	**Dotyczy faz S_5, S_6, S_7**
	
	
	

Źródło: opracowanie własne.

Użycie pakietu Vensim® wymagało wcześniejszego zdefiniowania układu równań w języku dynamiki systemowej.

Podsumowanie

Zdefiniowany w pracy ogólny cykl ataku wyróżnia się od publikowanych w literaturze[17] opisów cyklu życia ataku cybernetycznego dodanymi dwoma fazami: identyfikacji potrzeb atakującego oraz zakończenia ataku. Ponadto, w odróżnieniu od dotychczasowego ujęcia przez innych badaczy, w przyjętym w pracy cyklu życia ataku czyn-

[17] Coleman, 2012; Hutchinsi in., 2011; Hahn i in., 2015; Spring, Hatleback, 2017; Khan i in., 2018.

ności: a) uruchomienie, b) ewentualna instalacja kodu złośliwego oraz c) dowodzenie, kierowanie i sterowanie występują jako jedna faza. Takie ujęcie umożliwia rozważanie tej właśnie fazy jako wyodrębnionego cyklu życia, nie tracąc jednocześnie całego procesu ataku z pola widzenia.

Z uwagi na to, że do tej pory w dostępnych źródłach nie publikowano stochastycznego modelu cyklu życia cyklu ataku, w tym miejscu wypełniamy tę lukę proponując model na bazie łańcucha Markowa z ciągłym parametrem czasu.

Na bazie tak sformułowanego modelu, wyliczone charakterystyki probabilistyczne, takie jak: prawdopodobieństwa przebywania w poszczególnych fazach, czasy trwania poszczególnych faz czy też czas do pierwszej kompromitacji systemu, można wykorzystać na potrzeby szacowania ryzyka i zarządzania bezpieczeństwem organizacji i świadczonych e-usług (Stanik, Hoffmann, 2017).

Literatura

Coleman, K.G.J. (2012). Aggresssion in Cyberspace. W: Jasper S. (red.), *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security* (s. 105–119). Washington, DC: Georgetown University Press.

Hahn, A., Thomas, R.K., Lozano, I., Cardenas, A. (2015). A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*, *11*, 39–50.

Hutchins, E.M, Cloppert, M.J, Amin, R.M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.* Pobrano z: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf: Lockheed Martin.

Khan, M.S., Siddiqui, S., Ferens, K. (2018). A Cognitive and Concurrent Cyber Kill Chain Model. W: Daimi K. (red.), *Computer and Network Security Essentials.* Cham, Switzerland: Springer.

Lawler, G.F. (2006). *Introduction to Stochastic processes*. London–New York: Chapman and Hall/CRC Taylor and Francis Group.

Stanik, J., Hoffmann, R.(2017), *Model ryzyka procesów biznesowych*, W: Ekonomiczne Problemy Usług, 1/2017 (126), (s. 325-338), Szczecin: Uniwersytet Szczeciński.

Spring, J.M., Hatleback, E. (2017). Thinking about intrusion kill chains as mechanisms. *Journal of Cybersecurity*.Pobrano z: https://doi.org/10.1093/cybsec/ tyw012: Oxford Academic.

THE GENERAL CYBER-ATTACK LIFE CYCLE AND ITS CONTINUOUS-TIME MARKOV CHAIN MODEL

Keywords: cyber-attack process, cyber-attack life cycle, Continuous-Time Markov Chain, Markov process with countable state spaces

Summary. The article proposes a general cyber-attack life cycle which is distinguished from those published in the literature in principle by two additional phases: identifying attackers' needs and ending a cyber-attack. On the basis of the defined attack life cycle, a stochastic model describing its functioning was presented. The model is based on stationary Continuous-Time Markov Chains.

Translated by Romuald Hoffmann

Cytowanie

Hoffmann, R. (2018). Ogólny cykl życia ataku cybernetycznego i jego markowowski model, *Ekonomiczne Problemy Usług, 2* (131/1), 121–130. DOI: 10.18276/epu.2018.131/1-12.