JOURNAL OF MODERN SCIENCE
TOM 3/52/2023
www.jomswsge.com

DOI: doi.org/10.13166/jms/173091

Małgorzata Poniatowska-Jaksch
Warsaw School of Economics, Poland
Email: mponia@sgh.waw.pl
ORCID: 0000-0001-5737-655X

ZAGROŻENIE ATAKIEM ZŁOŚLIWYM OPROGRAMOWANIEM RANSOMWARE W EUROPE

THREAT OF RANSOMWARE ATTACK IN EUROPE

Abstract

A negative consequence of the digitization of the economy is the development of digital crime, and in this group a ransomware attack in the Ra aS model is a very high threat. The aim of the article is an attempt to determine the scale and identification of directions (sectors) of ransomware attacks in 11 EU countries in connection with the integration of digital technologies by enterprises and the level of social digital competence. The separation groups of countries into those with a high, medium and low level of ransomware made it possible to use the authorial synthetic indication constructed on the basis of the taxonomic method of development pattern (Sophos, Comparitech, DESI database). The research shows the luck of interdependence between synthetic indicator of ransomware and the variables considered to be key signs of the progressing digitization of the economy. The most vulnerable sectors to attack are: business, government administration and the health sector.

In Europe, a ransomware attack is determined by the ability to obtain a high ransom, therefore organizations with a high willingness to pay for fear of losing their reputation, become the greatest target. The choice of an organization – a potential victim of an attack, is not affected by its IT level or digital competences of employees. The platform model adopted by cybercriminals, is characteristic of global technology companies, whose the basis for success is advanced technologies and above-average digital competence of employees. RaaS model appears to be a major challenge for cybersecurity in the 21st century.

Streszczenie

Negatywną konsekwencją cyfryzacji gospodarki jest rozwój przestępczości cyfrowej, a w tej grupie bardzo dużym zagrożeniem jest atak złośliwym oprogramowania ransomware w modelu RaaS. Celem artykułu jest próba określenia skali i identyfikacja kierunków (sektorów) ataków ransomware w 11 państwach UE w powiązaniu z integracją technologii cyfrowych przez przedsiębiorstwa i poziomem społecznych kompetencji cyfrowych. Wydzielenie grup państw o wysokim, średnim i niskim poziomie zjawiska ransomware umożliwiło zastosowanie autorskiego syntetycznego wskaźnik skonstruowanego na podstawie taksonomicznej metody wzorca rozwoju (baza danych Sophos, Comparitech, DESI). Z badań wynika, że nie występują współzależności pomiędzy syntetycznym wskaźnikiem ransomware a zmiennymi, uznawanymi za kluczowe przejawy postępującej cyfryzacji gospodarki. Najbardziej narażone sektory na atak to: biznes, administracja rządowa i sektor zdrowia.

W Europie o przeprowadzeniu ataku ransomware decyduje możliwość uzyskania wysokiego okupu, co czyni celem ataku organizacje o dużej skłonności do jego uiszczenia w obawie o utratę reputacji. Na wybór organizacji – potencjalnej ofiary ataku, nie ma wpływu jej poziom IT ani kompetencje cyfrowe pracowników. Przyjęty przez cyberprzestępców model platformy, charakterystyczny dla globalnych firm technologicznych, gdzie podstawą sukcesu są zaawansowane technologie i ponadprzeciętne kompetencje cyfrowe pracowników jawi się dużym wyzwaniem dla cyberbezpieczeństwa w XXI w.

Keywords: *digitalization, economy, phishing, ransomware, cybersecurity*

Słowa kluczowe: *cyfryzacja, gospodarka, phishing, ransomware, cyberbezpieczeństwo*

Wprowadzenie

Rewolucja cyfrowa wraz z towarzyszącymi jej narzędziami technologicznymi legły u podstaw Nowej Gospodarki Cyfrowej (NGC), której podstawowymi wyznacznikami są platformy i dane. W oparciu o nie dokonuje się cyfrowa społeczno-gospodarcza transformacja, której towarzyszy nasilenie przestępczości cyfrowej. Za jedno z największych zagrożeń dla cyberbepieczeństwa uznawany jest ransomware. Jest to złośliwe oprogramowanie blokujące dostęp do urządzenia (komputera, smartfonu) w celu wyłudzenia okupu za klucz deszyfrujący. Początki ransomware sięgają lat 80. XX w., gdy pocztą były wysyłane zawirusowane dyskietki, wraz z zaproszeniem do wypełnienia ankiety oceniającej ryzyko zarażenia się AIDS. Do ok. 2015 ataki ransomware były prowadzone przez grupy przestępcze, które rozsyłały własny kod szyfrujący (Lewis, 2018, s. 11). W XXI w. cyberprzestępcy nie muszą już pisać własnych programów, lecz mogą skorzystać z usług specjalizujących się w tym zakresie platform cyfrowych (eSentire, 2023).

Uchwycenie ransomware jest niezwykle trudne, gdyż znaczna większość ataków nie jest ewidencjonowania (ENISA, 2022, s. 3). Niemniej jednak wzrost cyberprzestępczości wiąże się z postępującą cyfryzacją życia społeczno-gospodarczego, której negatywnym aspektom ma m.in. przeciwdziałać przyjęta przez Komisję Europejską *Strategia bezpieczeństwa cybernetycznego*. (European Commision, 2020). Celem artykułu jest próba określenia skali i identyfikacji kierunków (sektorów) ataku ransomware w państwach UE w powiązaniu z integracją przez przedsiębiorstwa technologii cyfrowych i poziomem społecznych kompetencji cyfrowych. U podstaw rozważań znajduje się hipoteza, że w UE ataki ransomware w pierwszej kolejności kierowane są do organizacji w sektorach najsłabiej zabezpieczonych i/lub skłonnych zapłacić okup w celu ochrony reputacji. Ich wzrost wnika z przeprowadzenia ataku w modelu RaaS, który obniżył bariery wejścia do przeprowadzania ataków, a postępująca integracja technologii cyfrowych wykorzystywanych przez organizacje, jak i wzrost społecznych kompetencji cyfrowych w UE nie są gwarantem bezpieczeństwa.

Metody badawcze

Zastosowana metodologia badawcza składa się z czterech etapów.

Pierwszy etap – przegląd literatury identyfikujący przyczyny rozwoju i specyfikę ataków złośliwym oprogramowaniem ransomware.

Drugi etap – na podstawie taksonomicznej metody wzorca rozwoju, wykorzystywanej do oceny poziomu zróżnicowania obiektów (Stec, 2013, s. 64-81) ocena skali zjawiska ransomware w wybranych wysoko rozwiniętych krajach UE tj.: Austrii, Polsce, Republice Czeskiej, na Węgrzech, Belgii, Francji, Hiszpanii, Holandii, Szwecji, Niemczech i we Włoszech w latach 2018-2022. Skonstruowany w tym celu algorytm badawczy, dający podstawę wydzielenia grup państw o wysokim, średnim i niskim poziomie zjawiska ransoware obejmował następujące kroki:

1. Dobór zmiennych uwzględniających kryteria stosowane w badaniach przestrzennych.
2. Rozpoznanie zmiennych diagnostycznych, spośród których 9 z 10 okazało się stymulantami.
3. Określenie niezależności wybranych cech wyznaczając współczynnik korelacji liniowej Pearsona pomiędzy wszystkimi zmiennymi, co pozwoliło na wyeliminowanie cech wzajemnie silnie skorelowanych. Jako kryterium silnego skorelowania zmiennych przyjęto r≥0,7. W wyniku analizy korelacji w dalszym badaniu pominięto trzy zmienne skorelowane, co oznaczało, że w do oceny wskaźnika syntetycznego wykorzystano łącznie siedem z 10 zmiennych.
4. Standaryzacja zmiennych w celu uzyskania porównywalności zmiennych przeprowadzona z wykorzystaniem wzoru:

$$z_{ik} = \frac{x_{ik} - \overline{x}_k}{S_k} \; ; S_k = \left[\frac{1}{w}\sum_{i=1}^{w}(x_{ik} - \overline{x}_k)^2\right]^{\frac{1}{2}}$$

gdzie:

w – liczba jednostek (kraj) ,

w_{ik} –wartość k-tej zmiennej w i-tej jednostce,

$\overline{x}_k$ – średnia arytmetyczna k-tej zmiennej,

S_k – odchylenie standardowe k-tej zmiennej,

z_{ik} – standaryzowana wartość k-tej zmiennej w i-tej jednostce.

5. Wyznaczenie wzorca P_0, w niniejszym badaniu najmniej dotkniętego atakami i ich skutkami, tj. łączącego wszystkie najlepsze cechy badanych jednostek. Podstawę jego skonstruowania stanowi znormalizowana macierz cech (Z) poprzez określenie wektora P_0, gdzie:

$$P_0 = [z_{01}, z_{02}, \dots z_{0s}, \dots z_{01}],\ z_{0s} = \max_i z_{is} \Rightarrow s \in Iz\_0s = (min) \neg i\ z\_is \Rightarrow s \notin I$$

6. Obliczenie odległości taksonomicznych, pomiędzy badanymi jednostkami (państwami) a wzorcem.

$$c_{i0} = \left[\sum_{s=1}^{n} (z_{is} - z_{0s})^2\right]^{\frac{1}{2}}$$

gdzie:
n – liczba cech,
z_{is} – wartość s-tej zmiennej w i-tej jednostce.

5. Wyznaczenie miary di* na podstawie odległości taksonomicznych:

$$d_i^* = \frac{c_{i0}}{c_0}, \text{ gdzie } c_0 = \overline{c}_0 + 2S_0, \overline{c}_0 = \frac{1}{w}\sum_{i=1}^{w} c_{i0}, S_0 = \left[\frac{1}{w}\sum_{i=1}^{w}(c_{i0} - \overline{c}_0)^2\right]^{\frac{1}{2}}$$

Wskaźnik di mieści się w przedziale 0–1 i im bardziej wartość miary zbliża się do zera tym dana jednostka reprezentuje bliższy wzorcowi poziom badanego zjawiska.

Trzeci etap – weryfikacja zależności pomiędzy poziomem wskaźnika syntetycznego di zjawiska ransomware a zmiennymi, które uznawane są za kluczowe przejawy postępującej cyfryzacji gospodarki, rzutujące na zakres rozprzestrzeniania się m.in. ransomware. Za zmienne te w niniejszym badaniu przyjęto poziom: 1) integracji technologii cyfrowych, obejmującym co najmniej podstawową intensywność cyfrową, absorpcję przez przedsiębiorstwa wybranych technologii oraz handel elektroniczny oraz 2) kompetencji cyfrowych w badanych państwach, wyrażonym a) odsetkiem użytkowników Internetu z co najmniej podstawowymi umiejętnościami tworzenia treści cyfrowych, b) wskaźnikiem kapitału ludzkiego, uwzgledniającym odsetek specjalistów ICT.

Do skonstruowania wskaźnika syntetycznego zjawiska ransomware wykorzystano bazy danych Sophos (2022) oraz Comparitech (Moody, 2023), a do oceny poziomu cyfryzacji w badanych krajach dane DESI (European Commision, 2022).

Kluczowe czynniki wzrostu ataków ransomware

W przypadku ataku najczęściej wykorzystywanym kanałem dystrybucji złośliwego oprogramowania ransomware jest poczta elektroniczna. Szacuje się, że ponad 90% złośliwego oprogramowania jest dostarczane poprzez e-mail (Ahlgren, 2023). Hakerzy wykorzystują to podejście w oszustwach phishingowych, polegających na nakłonienia potencjalnej ofiary do zainstalowania złośliwego oprogramowania. Phishing definiuje się także jako działanie polegające na tworzeniu repliki istniejącej strony internetowej w celu nakłonienia użytkownika do podania danych osobowych, finansowych lub hasła (Merwe i in., 2005, s.1). To przekierowanie na fałszywą stronę nazywane bywa także pharming, a repliki stron www nie omijają technologicznych gigantów takich jak: Facebook, Google, czy Microsoft (Ahlgren, 2023).

Wzrost zagrożenia atakiem ransomware wynika z postępującej:

- cyfryzacji relacji społecznych, który to trend znacznie wzmocniła pandemia. Społeczne potrzeby w coraz większym stopniu zaspokajane są *przez dostępność* bez wychodzenia z domu jak: zakupy przez Internet, płatności on-line, e-wizyta u lekarza. Zachodzą też istotne zmiany na rynku pracy (Svistunov i in., 2020, s.513-522) – rozpowszechnienie pracy zdalnej. Na cyfryzację relacji społecznych wpływ ma też wejście w wiek aktywności zawodowej tzw. pokolenia sieci. Do cech tego pokolenia należy zaliczyć dużą aktywność w życiu prywatnym i zawodowym w sieci oraz nadmierne zaufanie do cyfrowych ekosystemów (Pakulska i Poniatowska-Jaksch, 2021, s. 24-25), co jest wykorzystywane przez cyberprzestępców. Ofiarami ransomware najczęściej są użytkownicy Windows i internauci oszukani podczas poszukiwania informacji, korzystający z mediów społecznościowych (Jereth, 2021), czy bankowości elektronicznej.

- cyfryzacji relacji biznesowych. Rozwój Internetu pociąga za sobą istotne zmiany w realizowanych modelach biznesu – coraz częściej mają one charakter wirtualny. Postępująca wirtualizacja przedsiębiorstw reprezentujących gospodarkę tradycyjną to zaś nowe możliwości w kształtowaniu przewagi konkurencyjnej u podstaw, której znajdują się: sieciowe relacje biznesowe, interaktywna komunikacja z klientem, czy też kreacja otwartych innowacji (Pakulska, 2017, s.39-54). Na poziomie biznesu przedsiębiorstwa należy postrzegać jako mniej lub bardziej otwarte ekosystemy platformy.
- rozwoju e-administracji publicznej, w której w początkowym okresie największą wagę przy-wiązywano do zwiększenia efektywności i zmniejszenie kosztów jej funkcjonowania. Na bardziej zawansowanym etapie działań e-administracja ukierunkowania jest na wzmocnienie demokracji poprzez zwiększenie partycypacji wszystkich jej uczestników (Kusiak-Winter, 2021, s. 15-27). Wiąże się to z jej większą cyfrową *otwartością* poprzez wykorzystanie do komunikacji mediów społecznościowych i większej liczby otwartych baz danych na portalach administracji publicznej (Lee i Kwak, 2012, s.492-503).

W efekcie w drugiej dekadzie XXI w. platformy spotykane są we wszystkich sektorach gospodarki (Kenney i in., 2019, s. 871–879), a Kenney i Zysman (2016, s.61-69) nasilającą się *platform economy* porównują wręcz do nowej rewolucji przemysłowej. Nowe technologie wykorzystywane na platformach umożliwiają gromadzenie, wykorzystywanie i analizowania dużych zbiorów danych, śladów wirtualnej aktywności osobistej, społecznej i biznesowej. Kontrola nad danymi umożliwia platformom transformację w inteligencję cyfrową, co ma obecnie strategicznie znaczenie w rozwoju firm i całych gospodarek na świecie. Z potęgi władzy nad *danymi* zdają sobie sprawę zarówno rządzący, jak i rozwijający się w ekosystemach platformy świat przestępczy.

Do korzystania z usług platformy wystarczy Internet, komputer (coraz częściej smartphone) oraz kompetencje cyfrowe. Te ostatnie to zbiór wiedzy, umiejętności i postaw niezbędnych do aktywnego uczestnictwa w życiu społecznym. Ramy kompetencji cyfrowych 2.0. zostały określone przez Komisję Europejską i to dzięki nim coraz sprawniej poruszamy się w wirtualnej

sieci. Kompetencje cyfrowe możemy nabyć w sposób formalny – kursy szkolenia i nieformalny (Seufert i Scheffler, 2016, ss. 50-65; Treglia i Tomassoni, 2019, s. 55-60). Badania potwierdzają, że nawet korzystanie z wikipedii może podnieść nasze kompetencje cyfrowe (Petrucco, 2010, s.29-35), lecz ich poziom w tym przypadku nie jest wysoki, a zwłaszcza w kwestii bezpieczeństwa. W opublikowanym przez KnowBe2022 raporcie Phishing by Industry Report 4 stwierdzono, że jedna trzecia wszystkich pracowników nie przeszła testu phishingowego i prawdopodobnie otworzy podejrzaną wiadomość e-mail lub kliknie w podejrzany link (Ahlgren, 2023). Z drugiej strony wysoki poziom kompetencji cyfrowych obserwujemy w grupie cyberprzestępców.

Ransamware jako model platformy

Atakującymi mogą być indywidualni użytkownicy, pojedyncza grupa przestępców, ale najbardziej perspektywicznym w tym przekroju modelem jest Ransomware as-a-Service (RaaS). Cechy modelu RaaS jako platformy sprawiły, że złośliwe oprogramowanie w ciągu ostatniej dekady było rozpowszechniane w tempie wykładniczym i w 2021 r. zostało ocenione przez ENISA jako główne zagrożenie dla cyberbezpieczeństwa dla całej UE (ENISA, 2022, s. 6).

RaaS obniżył bariery wejścia do przeprowadzania ataków złośliwym oprogramowaniem ransomware. Atakujący nie muszą już potrafić napisać oprogramowania ransomware, a jedynie wiedzieć, jak przeprowadzić atak. Odpowiednie oprogramowanie udostępniają platformy RaaS. Pojęcie *platforma* jest niejednoznaczne (Parker, Van Alstyne i Choudary, 2016, s. 4-5). Przyjmując za Gawer (2014, s. 1239–1249) platformy to ewoluujące organizacje, które: 1) zrzeszają oraz koordynują działania innowacyjnych i konkurujących ze sobą agentów (w tym również cyberprzestępców); 2) tworzą wartość po stronie podażowej i/lub popytowej rynku; 3) mają modułową architekturę, którą tworzy rdzeń i peryferia. W definicję tą wpisuje się RaaS, gdyż operatorzy oprogramowania ransomware nie są już pojedynczymi podmiotami, ale tworzą złożony ekosystem dostawców i dostawców pomocniczych, którzy wymieniają się usługami w sieci. Poza zbiorem podmiotów bezpośrednio zaangażowanych we wdrażanie oprogramowania ransomware (rdzeń platformy),

szerszy ekosystem obejmuje dalszych graczy po stronie ofiary (peryferia platformy), które mogą czerpać zyski z ataków ransomware. Należą do nich (Clancy, 2021):

- firmy zajmujące się pomocom ofiarom ataku w zakresie reagowania na incydenty;
- brokerzy oprogramowania ransomware, których działania obejmują: negocjacje, obsługę płatności w imieniu ofiary itp.;
- ubezpieczyciele;
- prawnicy.

RaaS jest platformą technologiczną – grupa technologii, które są podstawą opracowywania innych aplikacji, procesów lub technologii (Gawer i Cusumano, 2014, s. 649-656). Pozwala ona autorom programów ransomware znacznie rozszerzyć skalę i zasięg działania, udostępniając kod do ich dostępu prawie każdemu zainteresowanemu. Efekty skali prowadzą do szybkiego wzrostu zysku, przy nieznacznych kosztach (Hernandez-Castro, Cartwright i Stepanova, 2017, s. 1-14). Zamiast pojedynczego podmiotu lub grupy tworzącej oprogramowanie ransomware dla swoich indywidualnych potrzeb, model RaaS umożliwia autorom tworzenie platform, na których *podmioty stowarzyszone* mogą wdrażać je zgodnie z własnymi celami (Lewis, 2018, s. 12). Platformy RaaS wprowadzają również nowy poziom anonimowości do operacji cyberprzestępczych.

Model Raas, tak jak inne modele e-biznesu, umożliwia generowanie dochodu z wielu źródeł. Jednym nich jest % od okupu wypłacanego podmiotom stowarzyszonym, często 10-20% lub więcej. Innymi źródłami dochodu mogą być: sprzedaż danych w określonych celach, miesięczne subskrypcje, które podmioty stowarzyszone płacą za dostęp do platformy lub doradztwo na rzecz innych cyberprzestępców (ENISA, 2022, s.16-18). Bez względu na to, który model wybierze użytkownik, ma on zapewnioną łatwą i kompleksową obsługę. W ramach Raas obsługiwane są również rozliczenia, prowadzi się monitoring przebiegu ataku, przeprowadza się aktualizację oprogramowania i generuje raporty zwierające m.in. obliczenia i prognozy rachunku zysków i strat (Feilner, 2021).

W przypadku ataku złośliwym oprogramowaniem ransomware obserwuje się zmiany w kierunku modelu Data Brokering. W tym przypadku

cyberprzestępcy sprzedają wykradzione dane oferentom, którzy zaoferują najwyższą cenę. Data Brokering obejmuje również odsprzedaż uzyskanego dostępu do danych innym podmiotom w celu dodatkowego wykorzystania (ENISA, 2022, s.16-18).

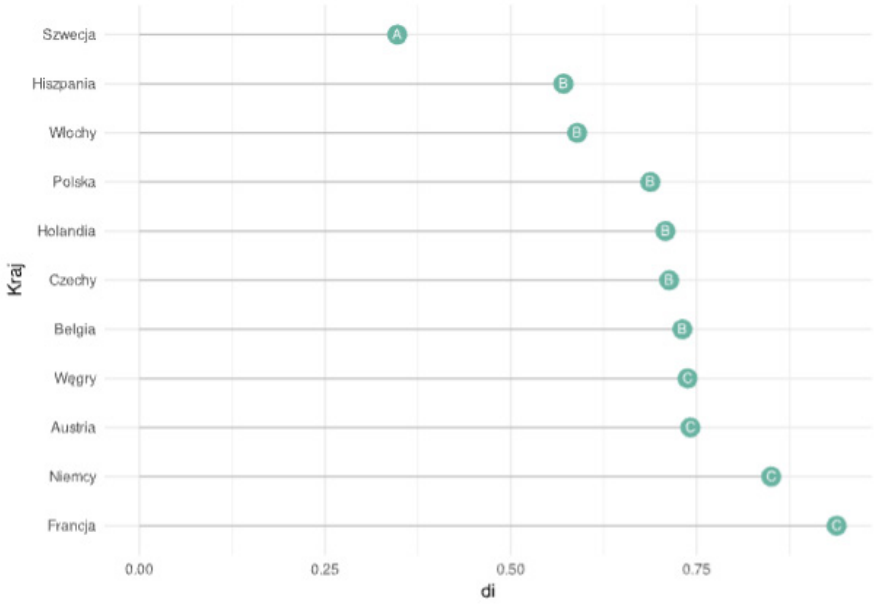
Operatorzy oprogramowania ransomware starają się zachować dobrą reputację, gdyż w przeciwnym razie ofiary nie zapłacą okupu. Wielu atakujących obiecuje, że po dokonaniu płatności usuną dane ofiar ze swoich baz i nie ujawnią ich publicznie. Z badań przeprowadzonych przez specjalistę ds. bezpieczeństwa cybernetycznego Venafi wynika jednak, że praktyka nie zawsze jest taka (Toulas, 2022).

Ataki ransomware w Europie – zróżnicowanie przestrzenne i sektorowe

Liczba ataków na świecie skalsyfikowanych jako ransomware 1) wykazuje tendencję wzrostową, która uległa istotnemu nasileniu w latach 2021-2022, zwłaszcza w 2021 r. (1365 ataków w 2021 i 795 w 2022 r. w stosunku do jeszcze relatywnie niewielkiego ich poziomu w 2018 r. (159 ataków) (Moody, 2023), 2) atakami objęte są w szczególności kraje wysoko ekonomicznie rozwinięte.

W grupie 11 poddanych badaniu państw europejskich z zastosowaniem wskaźnika syntetycznego zjawiska ransomware wynika, że najwyższy jego poziom jest charakterystyczny dla Francji, Niemiec, Austrii oraz Węgier (por. rys. 1).

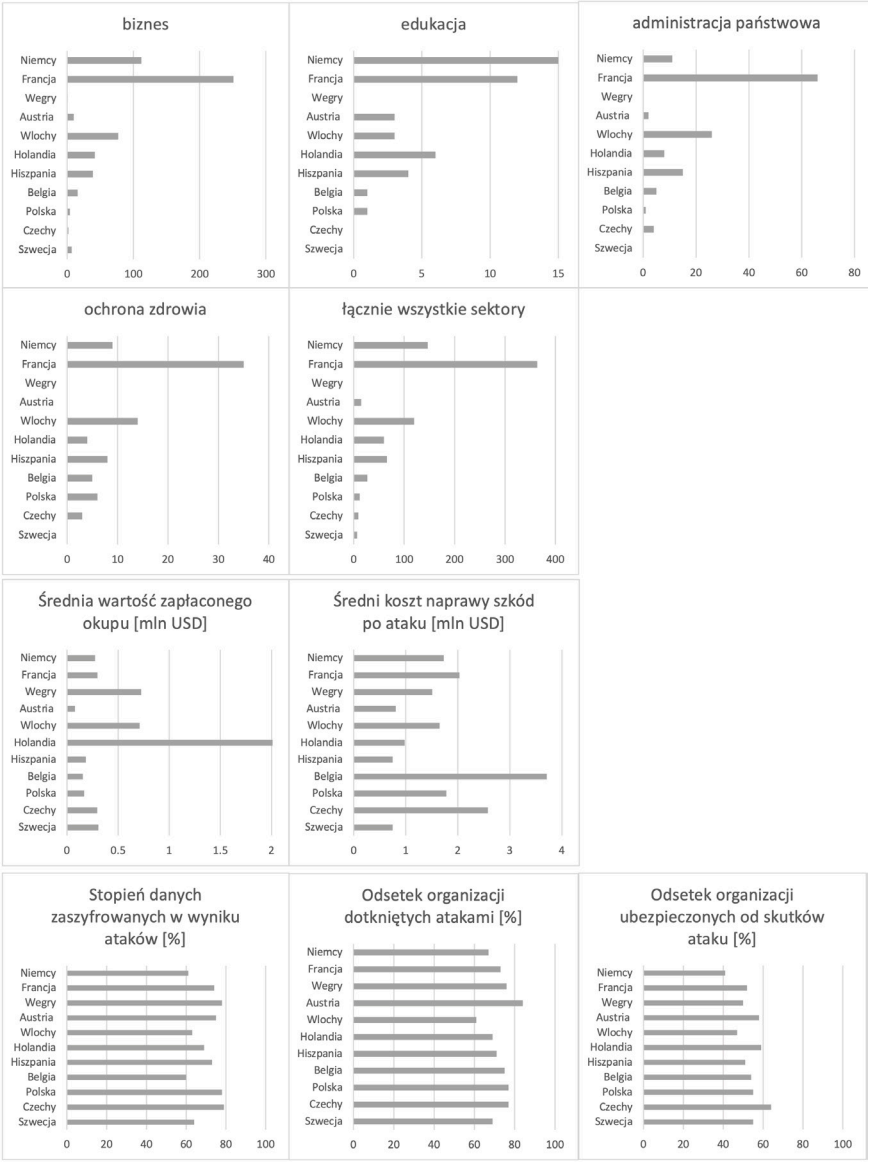
Rysunek 1. *Grupy badanych państw Europy według poziomu zagrożenia ransomware na podstawie syntetycznego wskaźnika di w 2022 r.*



Źródło: opracowanie własne na podstawie baz danych Sophos oraz Comparitech.

Na przeciwległym biegunie sklasyfikowano Szwecję, która wykazała najniższy poziom badanego zjawiska. Pozostałe państwa, tj. Hiszpanię, Włochy, Polskę, Holandię, Republikę Czeską oraz Belgię zaliczono do drugiej grupy, o średnim poziomie zagrożenia atakiem ransomware. Podział państw pod względem poziomu wskaźnika di znajduje odzwierciedlenie w zróżnicowanym wśród tych państw poziomie wskaźników cząstkowych – por. rysunek 2.

Rysunek 2. *Zagrożenie atakami ransomware w badanych państwach europejskich według wskaźników cząstkowych wskaźnika syntetycznego di w latach 2018-2022.*



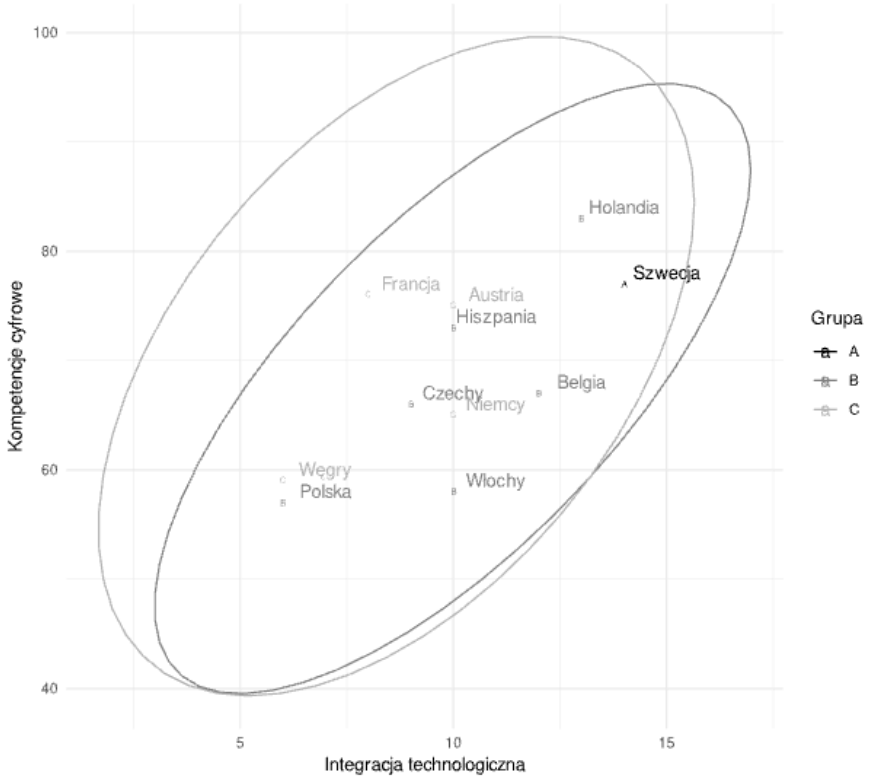
Źródło: opracowanie własne na podstawie bazy danych Sophos i Comparitech.

W ujęciu sektorowym na świecie najbardziej zagrożony atakami cybernetycznymi typu ransomware w 2022 r. był sektor biznesu (423 ataki), następnie administracja rządowa (151 ataków), opieka zdrowotna (117 ataków) oraz edukacja (104 ataki) (Moody, 2023). Biorąc pod uwagę liczbę rekordów objętych atakiem ransomware szczególnym przedmiotem ataków cyberprzestępców był sektor biznesu i służby zdrowia (odpowiednio 864 503 rekordów i 189 387 rekordów). Natomiast w sektorze administracji rządowej, a dopiero w dalszej kolejności w sektorze biznesu odnotowano najwyższą wartość wypłaconego okupu (średnio odpowiednio 9,8 mln USD i 7,8 mln USD).

Zbliżona do notowanej na świecie struktura sektorowa ataków ransomware jest także obserwowana w badanej grupie 11 państw w Europie. Największa ich liczbę w latach 2018-2022 odnotowano: w biznesie (560 ataków), administracji rządowej (138 ataków) i sektorze zdrowia (92 ataki), najmniej zaś w edukacji (45). Sektor biznesu i edukacji stał się przedmiotem największej liczby ataków we Francji oraz w Niemczech, a tego rodzaju najczęstsze praktyki w administracji rządowej i służbie zdrowia odnotowano poza Francją także we Włoszech. Szczególne zagrożenie charakterystyczne jest dla sektora medycznego, gdyż dokumentacja medyczna dla hakerów okazuje się być najważniejsza. Dokumentacja finansowa może zostać anulowana i ponownie wydana po wykryciu cyberataków. Dokumentacja medyczna pozostaje z osobą na całe życie (Ahlgren, 2023).

W grupie badanych 11 państw UE nie odnotowano zależności pomiędzy poziomem ataków ransoware a poziomem integracji technologii cyfrowej w podmiotach, które zostały nim dotknięte (wskaźnik korelacji Pearsona wyniósł – 0,49) – por. rys. 3. Jest to szczególnie istotne w warunkach relatywnie wysokich inwestycji ponoszonych na integrację technologii cyfrowych w państwach UE planowanych w obecnej dekadzie, w tym w zakresie wzrostu udziału firm MSP korzystających z chmury, sztucznej inteligencji i dużych zbiorów danych. Łączne środki na wsparcie cyfryzacji przedsiębiorstw sięgają w tym okresie 24 mld EUR a na prace B+R związane z wdrażaniem technologii cyfrowych i kompetencji cyfrowych kolejne 18 mld EUR, przy czym największe inwestycje charakterystyczne są dla Włoch, Hiszpanii, Niemiec i Grecji (European Commision, 2022, s.47).

Rysunek 3. *Zależność pomiędzy poziomem ataków ransomware w badanych państwach europejskich w 2022 r. na podstawie wskaźnika syntetycznego di a poziomem integracji technologicznej organizacji i kompetencji cyfrowych.*



Źródło: opracowanie na podstawie danych bazy danych Sophos, Comparitech oraz DESI.

Nie zachodził też istotny związek pomiędzy wielkością badanego zjawiska a zakresem cyfrowych kompetencji społecznych (wskaźnik Pearsona wyniósł – 0,49) i poziomem kapitału ludzkiego (-0,39). Najlepszym tego przejawem jest fakt, że w gronie państw w największym stopniu zaatakowanych ransomware wśród badanych, a także pozostałych państw UE znalazły się Francja i Niemcy, które w 2022 r. posiadały najwyższą liczbę osób pracujących jako specjaliści ICT (tj. 2 mln specjalistów ICT w Niemczech i 1,2 mln we Francji, tj. odpowiednio 22,5% i 13,9% siły roboczej ICT w UE). Łącznie z Włochami, które reprezentowały

średni poziom zagrożenia atakami na wskazane kraje przypadało ponad 40% siły roboczej ICT w UE, co skłania do przypuszczenia, że trudno te umiejętności cyfrowe jednoznacznie uznać za czynnik chroniący organizacje przed atakami.

Wnioski

Cyberprzestępczość jest nierozłącznym elementem rewolucji cyfrowej. W modelu RaaS jest ona opłacalna nie tylko dla samych twórców oprogramowania ransomware, ale dla całego ekosystemu platformy zarówno po stronie atakujących, jak i ofiar. Wyniki badania jednoznacznie wskazują, że cyberprzestępcy dokonując ataków złośliwym oprogramowaniem ransomware nie kierują się oceną jakości stosowanych w organizacjach rozwiązań IT i trudnością ich *przełamania* ani też poziomem cyfrowych kompetencji pracowników. Teoretycznie te ostatnie przesądzają nie tylko o skali absorpcji i wykorzystaniu cyfrowych technologii kluczowych dla funkcjonowania organizacji (analiza dużych zbiorów danych, usługi w chmurze i sztuczna inteligencja), ale też wpływają na cyberbezpieczeństwo organizacji. W Europie o przeprowadzeniu ataku ransomware decyduje jednak możliwość uzyskania wysokiego okupu, co czyni celem ataku organizacje o dużej skłonności do jego uiszczenia w obawie o utratę reputacji. Na wybór organizacji – potencjalnej ofiary ataku, nie ma wpływu jej poziom IT ani kompetencje cyfrowe pracowników. W Europie najbardziej narażone sektory na atak to: biznes, administracja rządowa i sektor zdrowia.

W świetle powyższych spostrzeżeń powstaje pytanie w jaki sposób można zabezpieczyć się przez cyberprzestępczością rozwijającą się w modelu platformy tj. modelu charakterystycznego dla globalnych firm technologicznych, w przypadku których podstawą sukcesu są: zaawansowane technologie oraz bardzo wysokie kompetencje cyfrowe pracowników (tym przypadku RaaS cyberprzestępców).

References

Ahlgren, M. (2023). 50+ Cybersecurity Statistics, Facts & Trends for 2023. Dostęp 22.05.2023 z: https://www.websiterating.com/research/cybersecurity-statistics-facts/

Clancy, M. (2021). Introducing the Ransomware Economy. Pobrano 11.05.2023 z: https://www.backblaze.com/blog/ransomware-economy/

ENISA (2022). Threat landscape for ransomware attacks. Pobrano 10.05.2023 z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

eSentir (2023). Stop It Before It Spreads. Pobrano 11.05.2023 z: https://www.esentire.com/how-we-do-it/use-cases/ransomware?utm_source=pardot&utm_medium=e-mail&utm_campaign=nurture&utm_content=ransomware-page&utm_medium=e-mail&utm_source=pardot&utm_campaign=prospect_nurture

European Commision (2022). Digital Economy and Society Index (DESI) 2022. Dostęp 24.04.2023 z: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022

European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade. Brussels.

Evans P. C., Gawer A. (2016). The Rise of the Platform Enterprise: A Global Survey. The Emerging Platform Economy Series.

Feilner, M. (2021). "Ransomware as a Service" as a Business Model: Why the Business of Extortion Flourishes. Pobrano 13.04.2023 z: https://www.greenbone.net/en/blog/ransomware-as-a-service/

Gawer, A. (2014). Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework, 43(7), 1239–1249. Research Policy.

Gawer, A., Cusumano, M.A. (2014). Platforms and Innovation. w: Dodgson, D.M. Gann, N. Phillips (ed.), The Oxford Handbook of Innovation Management, 649 -656. Oxford University Press,

Hernandez-Castro,J., Cartwright, E., Stepanova, A. (2017), Economic Analysis of Ransomware, 1-14. Political Economy: Government Expenditures & Related Policies eJournal. Pobrano 18.04.2023 z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937641

Jereth. (2021). Forget the dark web: ransomware gangs weaponize social media to pressure victims. Pobrano 18.05.2023 z: https://www.emsisoft.com/en/blog/39389/forget-the-dark-web-ransomware-gangs-weaponize-social-media-to-pressure-victims/

Kenney, M., Rouvinen, P., Seppälä, T., Zysman, J. (2019). Platforms and industrial change, 26(8), 871–879. Industry And Innovation.

Kenney, M., Zysman, J. (2016). The rise of the platform economy. 32(3), 61-69. Issues in Science and Technology.

Kusiak-Winter, R. (2021). Kierunki i etapy rozwoju e-administracji publicznej. w: R. Kusiak-Winter, J. Korczak (red.), Ewolucja elektronicznej administracji publicznej,

15-27. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

Lee, G., Kwak, Y.H. (2012). An Open Government Maturity Model for Social Media-Based Public Engagement, 29(4), 492-503. Government Information Quarterly.

Lewis, J. (2018). Economic Impact of Cybercrime - No Slowing Down. Dostęp10.05.2023 z: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic--impact-cybercrime.pdf

Moody, R. (2023). Map of worldwide ransomware attacks. Dostęp 23.05.2023 z: https://www.comparitech.com/blog/information-security/global-ransomware-attacks/

Pakulska, T. (2017). Otoczenie przedsiębiorstw w sharing economy. w: M. Poniatowska-Jaksch, R. Sobiecki (red.), Gospodarka współdzielenia, 39-54. OW SGH.

Pakulska, T., Poniatowska-Jaksch, M. (2021). Platformizacja korporacji transnarodowych. OW SGH.

Parker, G. G., Van Alstyne, M. W., Choudary S. P. (2016). Platform Revolution: How Networked How Networked Markets Are Transforming the Economy - and How to Make Them Work for You. W.W. Norton & Company Inc.

Petrucco, C. (2010). Wikipedia as Training Resource for Developing Digital Competences.,1(3), 29-35. International Journal of Digital Literacy and Digital Competence.

Seufert,S., Scheffler, N. (2016). Developing Digital Competences of Vocational Teachers, 7(1), 50-65. International Journal of Digital Literacy and Digital Competence.

Sophos (2022). The State of Ransomware 2022. Poprano 18.04.2023 z: https://www.sophos.com/en-us/whitepaper/state-of-ransomware

Stec, M. (2013). Wielowymiarowa analiza porównawcza zrównoważonego rozwoju krajów Unii Europejskiej, 58(3), 64-81. Przegląd Statystyczny.

Svistunov, V. M., Grishaeva, S. A., Konovalova, V. G. (2020). Labour Market in Digital Economy: New Opportunities, Requirements and Threats. w: V. V. Mantulenko (red.), Problems of Enterprise Development: Theory and Practice 82, 513-521. European Proceedings of Social and Behavioural Sciences. European Publisher.

Toulas, B. (2022). Ransomware extortion doesn't stop after paying the ransom. Pobrano 8.05.2023 z: https://www.bleepingcomputer.com/news/security/ransomware-extortion-doesnt-stop-after-paying-the-ransom/

Treglia, E., Tomassoni, R. (2019). The Development of Digital Competences and Emotional Skills Through the Use of Audio-Visual Technologies, 10(1), 55- 60. International Journal of Digital Literacy and Digital Competence.

v.d. Merwe, A., Look, M., Dabrowski, M. (2005). Characteristics and responsibilities involved in a Phishing attack. w: WISICT '05: proceedings of the 4th international symposium on information and communication technologies, 249–254. Trinity College Dublin.