ZESZYTY NAUKOWE
WYŻSZEJ SZKOŁY BANKOWEJ W POZNANIU
2023, T. 102, NR 3

MARCIN FUKSIEWICZ
Uniwersytet WSB Merito w Poznaniu
Wydział Zamiejscowy w Chorzowie
https://orcid.org/0000-0002-0811-1683
e-mail: fuksiewicz.marcin@gmail.com

Rodzaje i cechy charakterystyczne cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa

Streszczenie. Upowszechnianie się zaawansowanych technologii informatycznych powoduje, że coraz większym i powszechniejszym problemem stają się cyberataki na systemy komputerowe, serwery, programy, dane wrażliwe, smartfony czy elementy sieci komputerowych. Znajomość najbardziej typowych form cyberataków i metod obrony przed nimi powinna być jedną z podstawowych kompetencji pracowników przedsiębiorstw. Ponieważ typowy cyberatak przebiega zazwyczaj w kilku przewidywalnych krokach, kluczową rolę w każdym systemie cyberbezpieczeństwa odgrywają odpowiednio przeszkoleni i świadomi pracownicy, którzy jednocześnie stanowią jego największą wartość lub najsłabsze ogniwo. Nie bez znaczenia jest również świadomość skutków, w tym finansowych, typowego cyberataku dla przedsiębiorstwa.

Słowa kluczowe: cyberbezpieczeństwo, cyberatak, infrastruktura informatyczna, digitalizacja

https://doi.org/10.58683/dnswsb.615

1. Digitalizacja szansą i zagrożeniem

Rozwój technologii, w szczególności informatycznych, oddziałuje na podmioty o różnym zasięgu i wielkości, wpływa zarówno na pojedyncze jednostki, przedsiębiorstwa, jak i na społeczeństwa czy państwa. Powszechne użycie urządzeń elektronicznych w praktycznie wszystkich dziedzinach życia wymusza zmiany porównywalne do przemian ekonomicznych, technicznych, kulturowych i społecznych, jakie miały miejsce podczas rewolucji przemysłowych (Klich & Sochala, 2016). Zmiany te wymusiły powstanie globalnej sieci informatycznej i utworzenie społeczeństwa informacyjnego. Faktem stało się powstanie tzw. cyberprzestrzeni, łączącej świat technologii z różnymi grupami społecznymi (Michałkiewicz,

2016). Rozwój technologii — w szczególności komputerowych, dających szereg możliwości, w tym przewagę konkurencyjną i możliwość obniżenia kosztów czy skuteczniejszego zarządzania — idzie jednak w parze z rozmaitymi zagrożeniami. Ryzyko wystąpienia ataków cybernetycznych, mogących skutkować różnym zakresem strat, istnieje szczególnie w obszarze biznesu. Ataki na różnego rodzaju systemy informatyczne stanowią duże niebezpieczeństwo dla przedsiębiorstw niezależnie od ich rozmiaru. Są one poważnym zagrożeniem dla infrastruktury informatycznej, a ich skutki w zależności od skali i rodzaju mogą mieć różny zakres. Przedstawienie i zrozumienie procesów ataku cyberprzestępców jest niezwykle istotne, aby można skutecznie im zapobiegać. W dobie powszechnego korzystania w działalności biznesowej z technologii komputerowych ataki cybernetyczne stają się coraz większym wyzwaniem dla firm, instytucji, ale także osób fizycznych. Ważne staje się poznanie szeregu aspektów cyberbezpieczeństwa i przebiegu samych ataków cybernetycznych. Należy poszerzać wiedzę w zakresie najnowszych trendów z dziedziny cyberbezpieczeństwa, aby lepiej zrozumieć, jakie nowe rodzaje ataków mogą się pojawić oraz jak można się na nie przygotować. Zwiększenie świadomości na temat zagrożeń związanych z atakami cybernetycznymi oraz dostarczenie informacji i narzędzi, które pomagają w ochronie systemów komputerowych w różnego rodzaju organizacjach, umożliwi bezpieczniejsze i pewniejsze działania w środowisku cyfrowym (PBSG, 2021).

2. Co to jest cyberbezpieczeństwo

Obecnie wiele aspektów życia przeniosło się i cały czas się przenosi do świata cyfrowego, cyberbezpieczeństwo dotyczące przechowywania danych osobowych, wykonywania transakcji finansowych, komunikacji online i innych czynności staje się zatem warunkiem niezbędnym do prawidłowego funkcjonowania infrastruktury komputerowej. W miarę rozwoju technologii informatycznych i coraz większej zależności od systemów komputerowych, znajomość aspektów dotyczących zabezpieczeń staje się coraz bardziej paląca.

Czym zatem jest cyberbezpieczeństwo? Odnosi się ono do przeróżnych praktyk i procesów podejmowanych w celu ochrony systemów komputerowych, sieci, urządzeń i danych przed nieuprawnionym dostępem, uszkodzeniem, kradzieżą czy innymi formami ataków, gdzie krytyczną kwestią jest zapewnienie poufności, integralności i dostępności informacji oraz zachowanie prywatności użytkowników (Polska Bezgotówkowa, 2022).

3. Cyberazagrożenia dla infrastruktury informatycznej

Jak można natomiast zdefiniować cyberatak, określany również jako atak cybernetyczny? To działanie podejmowane przez jednostki lub grupy cyberprzestępców, którzy wykorzystują systemy i sieci komputerowe w celu naruszania bezpieczeństwa systemów komputerowych, sieci lub urządzeń, kradzieży czy zniszczenia danych. Ataki cybernetyczne mogą być wymierzone w różne elementy infrastruktury, zarówno w kontekście indywidualnych użytkowników, jak i firm czy instytucji. Cyberzagrożenia mogą dotykać każdego obszaru i procesu w firmie. Z uwagi na integrację systemów atak może dotyczyć działów sprzedaży, marketingu, obsługi klienta, kadr, finansów. Celami ataków mogą być przede wszystkim:

- aplikacje i oprogramowanie,
- urządzenia do przetwarzania informacji, jak na przykład komputery stacjonarne, laptopy,
- serwery, routery i inne urządzenia związane z przetwarzaniem danych,
- urządzenia mobilne, przede wszystkim smartfony czy tablety,
- sieci komputerowe i ich elementy,
- usługi chmurowe,
- działania pracowników, np. przypadkowo ujawniających hasła do komputera osobom trzecim.

Należy pamiętać, że powyższa lista nie jest wyczerpująca, jest to raczej zarys, a ataki cybernetyczne mogą być ukierunkowane na wiele innych elementów nie tylko infrastruktury informatycznej, ale również, co jest szczególnie ważne, sfery społecznej. Nie bez powodu mówi się, że ludzie w systemie cyberbezpieczeństwa są najsłabszym ogniwem. Ważne jest, aby zrozumieć, że każdy element infrastruktury cyfrowej, ale także korzystających z niej ludzi stanowi potencjalne zagrożenie i wymaga odpowiednich środków ochrony przed atakami.

4. Jakie rodzaje cyberataków grożą firmom

Firmy są narażone na różnorakie formy cyberataku, mogące mieć poważne konsekwencje dla ich działalności. Cyberataki mogą się różnić pod względem metodyki, celu i wykorzystywanych narzędzi. Niektóre z nich się przenikają lub uzupełniają w swoim działaniu. Przyjrzyjmy się najczęściej spotykanym rodzajom ataków cybernetycznych.

Ataki *ransomware*, polegające na zainfekowaniu systemów (np. firmy) złośliwym oprogramowaniem, które szyfruje znajdujące się tam dane, a następnie żąda okupu w zamian za ich odblokowanie. Ataki *ransomware* mogą paraliżować działalność firmy, powodując straty finansowe i utratę dostępu do ważnych danych.

Malware, skrót od *malicious software* (złośliwe oprogramowanie), to programy lub skrypty, które działają na komputerze bez zgody i wiedzy użytkownika, z korzyścią dla cyberprzestępców. Złośliwe oprogramowanie to wszelkiego rodzaju aplikacje i skrypty, które mają negatywny wpływ na komputer i jego użytkownika. Po uzyskaniu dostępu do sieci złośliwe oprogramowanie w postaci wirusów czy koni trojańskich wyrządza szereg szkód, blokując np. dostęp do danych, a w najgorszym przypadku przejmując kontrolę nad komputerem. Ataki tego typu obejmują także kradzież danych osobowych i informacji związanych z logowaniem do bankowości elektronicznej.

Ataki typu *man in the middle* (MITM) oznaczają, że cyberprzestępca, który próbuje włamać się do systemu, wkracza do komunikacji pomiędzy dwiema stronami i w sposób tajny zajmuje miejsce między nimi. Podmiot popełniający przestępstwo cybernetyczne jest zaangażowany w wymianę wszystkich wiadomości między stronami i podszywa się pod jedną z nich (np. stronę internetową banku lub skrzynkę pocztową). W ten sposób udaje zupełnie inną osobę i przechwytuje wrażliwe informacje.

Phishing to metoda oszustwa, w której cyberprzestępca również podszywa się pod inną osobę lub instytucję, starając się nakłonić odbiorcę do podjęcia określonego działania, na przykład otworzenia zainfekowanego linku lub pobrania dokumentu ze szkodliwym programem. Celem *phishingu* może być:

- wyłudzenie poufnych informacji, takich jak dane logowania czy numery kart kredytowych;
- zainfekowanie komputera szkodliwym oprogramowaniem;
- nakłonienie firmy lub pracowników do podejmowania określonych działań.

Ataki DDoS (*Distributed Denial of Service*) to jedne z najczęściej stosowanych ataków w sieci. Polegają one na zalewaniu np. serwerów ogromną ilością danych lub zapytań do bazy danych, pochodzących z setek tysięcy zainfekowanych komputerów z różnych miejsc na świecie. Taki ogromny przypływ danych powoduje, że serwery nie są w stanie przetworzyć informacji i przestają pracować z powodu obciążenia. Skutkiem tego cały system komputerowy zostaje sparaliżowany. W przypadku ataków DDoS strony internetowe ładują się bardzo wolno lub wcale, utrzymuje się brak dostępu do sieci, skrzynki e-mail zalewane są wiadomościami będącymi spamem, a łącza firmowe są całkowicie zablokowane.

SQL *Injection* to technika cyberataków, która polega na wstrzykiwaniu np. dodatkowych instrukcji do zapytania do bazy danych w celu ich wykonania. Ataki tego typu często dotyczą np. systemów obsługujących handel internetowy. Przez wykorzystanie luk w zabezpieczeniach aplikacji cyberprzestępca może zdobyć nieuprawniony dostęp do bazy danych i odnaleźć oraz wykraść dane klientów lub inne poufne informacje.

Atak *brute force*, inaczej nazywany atakiem siłowym, opiera się na wykorzystaniu łatwych do odgadnięcia haseł, które są używane np. w przedsiębiorstwach do logowania. Cyberprzestępcy tworzą specjalne oprogramowanie, które automatycznie tak długo próbuje różnych kombinacji haseł, aż znajdzie poprawne. Dzięki temu atakujący może uzyskać nieuprawniony dostęp do firmowych dokumentów. Ataki *brute force* wykorzystują fakt, że wiele osób nadal korzysta z prostych i łatwych do odgadnięcia haseł. Jeśli hasło jest słabe lub niewystarczająco złożone, atakujący może z łatwością je złamać i dostać się do poufnych informacji firmy. Dlatego ważne jest, aby pracownicy firm używali trudnych do odgadnięcia haseł i co określony czas je zmieniali. Pomocne jest też wprowadzanie wielopoziomowego uwierzytelnienia (np. poprzez dodatkowy kod SMS), co może dodatkowo zwiększyć bezpieczeństwo logowania.

Warto pamiętać, że zagrożenia dla bezpieczeństwa mogą pochodzić nie tylko z zewnątrz, ale również z wnętrza firmy. Przykładem takiego ataku jest sytuacja, gdy pracownik opuszcza przedsiębiorstwo, ale nadal ma kontakt z jego zasobami (np. aktywne konta, dostęp do aplikacji lub usług firmowych). Dlatego ważne jest zadbanie o usunięcie kont pracownika po jego odejściu oraz zmianę haseł do wszystkich usług, do których miał dostęp. Ataki wewnętrzne, zwane także *inside attack*, stanowią poważne zagrożenie dla firm. Były pracownik, posiadając nadal dostęp do systemów firmy, może naruszać poufność danych, dokonywać kradzieży informacji czy podejmować nieuczciwe działania. Takie środki ostrożności jak usuwanie kont byłych pracowników i regularna zmiana haseł mogą ograniczyć ryzyko potencjalnych ataków wewnętrznych (Polska Bezgotówkowa, 2021; PBSG, 2021; biznes.gov.pl, 2022).

Żeby zminimalizować ryzyko cyberataków, ważne jest zachowanie ostrożności i uważności, zwłaszcza podczas przeglądania wiadomości e-mail, klikania w linki na nieznanych stronach lub pobierania plików. Należy zawsze sprawdzać źródło wiadomości i być świadomym podejrzanych próśb o ujawnienie poufnych danych. Nie bez znaczenia pozostaje sfera społeczna, gdzie ludzie mogą stanowić najsłabsze ogniwo w ochronie infrastruktury informatycznej. Dodatkowo, korzystanie z programów antywirusowych i zabezpieczających może pomóc w wykrywaniu i blokowaniu części takich ataków.

5. Konsekwencje cyberataków

Konsekwencje cyberataków mogą być znaczne i dotykać różnych sfer naszego życia. Na poziomie jednostkowym ataki mogą prowadzić do kradzieży danych osobowych, medycznych, zasobów finansowych, co naraża użytkowników na ryzyko oszustw, utraty reputacji i naruszenia prywatności. Jeśli chodzi o firmy, ataki mogą powodować poważne straty finansowe, przerwy w działalności, utratę poufnych informacji biznesowych oraz uszczerbek wizerunkowy. W skrajnych przypadkach cyberataki mogą nawet zagrażać stabilności infrastruktury krytycznej państwa, takiej jak systemy energetyczne, transportowe czy opieki zdrowotnej, co ma poważne konsekwencje dla całych społeczeństw.

Efekty cyberataku można zauważyć zazwyczaj od razu poprzez paraliż infrastruktury informatycznej firmy. Przykładowo: brak dostępu do danych, problem z logowaniem do skrzynki pocztowej lub dostępem do chmury. Niektóre skutki ataków mogą być jednak subtelniejsze: spowolnienie urządzeń i aplikacji, niespodziewane usunięcie, zablokowanie plików lub folderów, a także wysyłanie spamu z zainfekowanych urządzeń. Ważne jest zatem zwrócenie uwagi na takie niepokojące sygnały, które mogą wskazywać na atak.

Ataki mogą skutkować stratami finansowymi, gdyż powodują niekiedy przerwy w działalności, co wiąże się z utratą przychodów. Dane udostępnione przez NASK pokazują, że aż dwie trzecie firm, które padły ofiarą cyberataków, doświadczyło znacznego spadku przychodów. Utrata lub uszkodzenie danych również generuje wysokie koszty. Często konieczna staje się naprawa uszkodzonego sprzętu lub infrastruktury, co niesie za sobą dodatkowe wydatki. W dłuższej perspektywie cyberataki mają negatywny wpływ na wizerunek firmy na rynku. Klienci i partnerzy mogą tracić zaufanie do organizacji, które nie są w stanie skutecznie chronić swoich danych. Zniszczenie reputacji może prowadzić do utraty klientów i potencjalnych kontraktów. Ponadto, skutkiem cyberataku może być utrata własności intelektualnej, takiej jak unikatowe patenty czy formuły, będące sekretem branżowym, które przyczyniały się do sukcesu firmy. Brak odpowiednich zabezpieczeń w internecie i działanie osób trzecich może skutkować nałożeniem kar administracyjnych, na przykład za naruszenie prywatności lub upublicznienie danych (biznes.gov.pl, 2023). Cyberataki mogą w najgorszym przypadku doprowadzić do bankructwa firmy. Dlatego nie można lekceważyć kwestii cyberbezpieczeństwa. Ważne jest, aby podejmować odpowiednie środki ochronne. Inwestycja w odpowiednie zabezpieczenia, szkolenie pracowników w zakresie świadomości cybernetycznej i utrzymanie wysokiego poziomu ochrony danych są niezbędne, aby chronić firmę przed negatywnymi skutkami ataków hakerskich (Polska Bezgotówkowa, 2022).

6. Ukryte koszty cyberataku i analiza skutków z perspektywy firmy

Jak wspomniano, cyberataki mogą mieć poważne konsekwencje dla różnych obszarów funkcjonowania przedsiębiorstwa. Ich wpływ może objawiać się w zakłóceniu operacji biznesowych, utracie danych, zepsuciu reputacji czy stratach finansowych. Koszty związane z cyberatakami są zróżnicowane i zależą od charakteru i wagi takiego zdarzenia. Wymagają one nakładów na naprawę systemów, odtworzenia utraconych danych, wzmocnienia zabezpieczeń oraz działań zapobiegawczych, a także mogą wiązać się z koniecznością wypłacenia odszkodowań klientom lub poniesienia kosztów naruszenia przepisów dotyczących np. ochrony danych.

Cyberataki często są postrzegane głównie przez pryzmat informacji, które są wykradane z przedsiębiorstw, zwłaszcza tych dotyczących danych osobowych, informacji o stanie zdrowia czy danych płatniczych. W kontekście finansowym dyskusje dotyczą przede wszystkim kwestii powiadomienia klientów o incydencie oraz potencjalnych spraw sądowych wytaczanych przez klientów lub kar nałożonych przez organy regulacyjne. Rzadko natomiast mówi się publicznie o przypadkach kradzieży własności intelektualnej, szpiegostwa, niszczenia danych, atakach na kluczowe operacje biznesowe lub próbach sparaliżowania infrastruktury krytycznej. Niemniej jednak tego rodzaju ataki mogą wywoływać znacznie poważniejsze konsekwencje dla organizacji i wiążą się z dodatkowymi kosztami, które trudno określić w prosty sposób, a opinia publiczna często się o tym dowiaduje. Aby zidentyfikować mniej oczywiste skutki cyberataku, konieczne jest zastosowanie wielodyscyplinarnego podejścia, które łączy głęboką wiedzę na temat tego rodzaju incydentów z kontekstem działalności firmy oraz technikami oceny i miarami finansowymi. Konsekwencje takiego ataku mogą się objawiać w różnym czasie i na różnych poziomach, podobnie jak w przypadku góry lodowej, gdzie widać tylko wierzchołek. Wśród kosztów ukrytych wyróżnić można następujące:

- wzrost składki ubezpieczeniowej,
- zwiększenie kosztów finansowania zewnętrznego,
- zakłócenie działalności operacyjnej,
- wartość utraconych przychodów z umów,
- koszty komunikacji z dostawcami i klientami,
- utratę reputacji,
- skutki zmian regulacji prawnych,
- skutki wprowadzonych działań naprawczych w zakresie IT,
- skutki działań naprawczych w obszarze bezpieczeństwa prawnego,

- koszty konsultacji w zakresie analizy po włamaniu,
- utratę zaufania do usług,
- utratę klientów,
- utracone relacje z klientami,
- dewaluację nazwy handlowej czy marki,
- utratę wartości intelektualnej,
- koszty usług prawnych.

Z powyższego zestawienia wynika, że ataki na zasoby firm mogą wywoływać długotrwałe i rozległe skutki. Dlatego kluczowym elementem ochrony przed cyberatakami i ich konsekwencjami jest pełne zrozumienie zależności pomiędzy posiadanymi zasobami a infrastrukturą, która je wspiera (CFO Insights, 2016).

7. Jak się zabezpieczać przed cyberatakami

Cyberbezpieczeństwo należy uznać za kluczowy czynnik zapewniający bezproblemowe działanie firmy. Konieczne jest inwestowanie w środki ochrony, które są adekwatne do potencjalnych zagrożeń. Ważnym elementem jest także przygotowanie właściwych procedur zabezpieczających oraz upewnienie się, że wszyscy pracownicy są odpowiednio poinformowani i tych procedur przestrzegają. Oczywiście wskazane jest także zapewnienie pracownikom całego systemu cyklicznych szkoleń.

Największe wydatki związane z cyberbezpieczeństwem dotyczą technologii. Niemniej jednak firmy mają szereg możliwości, aby posiadać podstawowe narzędzia bezpieczeństwa właściwie bez dodatkowych kosztów. Mniejsze wydatki wiążą się z opracowaniem polityki bezpieczeństwa firmy i przeszkoleniem pracowników.

Wnioski płynące z powyższych wskazań sugerują, że inwestowanie w cyberbezpieczeństwo to nie tylko kwestia kosztów, ale także ochrony przed potencjalnymi stratami i zagrożeniami dla firmy. Dbałość o bezpieczeństwo danych oraz świadomość pracowników w tym zakresie są kluczowe dla zabezpieczenia przed cyberatakami i minimalizowania potencjalnych szkód.

Ponieważ cyberbezpieczeństwo w firmie to także pracownicy, ważne jest inwestowanie w ich wiedzę, zwłaszcza poprzez szkolenia. Świadomość zagrożeń cybernetycznych powinna być szczególnie obecna u menedżerów i kadry zarządzającej. To oni mają za zadanie propagować tę świadomość wśród pracowników, którzy często stanowią najsłabsze ogniwo dla firmy w cyberprzestrzeni. Oto niektóre przykłady pokazujące to zjawisko:

- Jedna trzecia pracowników używa tego samego hasła na różnych platformach.
- Jedna czwarta zapomina zablokować komputer, gdy opuszcza biurko.
- Jedna piąta przechowuje hasła w widocznym miejscu, na przykład na kartce na biurku.

Należy zadbać, aby pracownicy mieli dostęp do aktualnych informacji o procedurach postępowania w przypadku cyberzagrożeń i cyberataków w firmie. Jeśli takowe procedury jeszcze nie istnieją, należy je opracować i wprowadzić. Najczęściej to administrator bezpieczeństwa danych lub specjalista IT, który może być pracownikiem firmy lub ekspertem zewnętrznym, jest odpowiedzialny za opracowanie polityki cyberbezpieczeństwa.

Istotne są również specjalistyczne szkolenia, które uczą, jak reagować na cyberataki, oraz prostsze szkolenia instruktażowe dotyczące metod zapobiegania cyberatakowi, dostępne dla każdej firmy, takie jak stosowanie silnych haseł i regularna ich zmiana, co właściwie powinny wymuszać same programy.

Regularne monitorowanie zabezpieczeń przed cyberprzestępczością w firmie jest niezwykle ważne. Można to osiągnąć poprzez systematyczne audytowanie używanego sprzętu i oprogramowania, sprawdzanie aktualności programów przeciwdziałających cyberzagrożeniom oraz weryfikację zmian haseł dostępowych.

Warto rozważyć zastosowanie bardziej zaawansowanych środków ochronnych, takich jak regularne audyty i zdobywane certyfikaty. Takie działania stanowią również dowód dla klientów, organów regulacyjnych i partnerów biznesowych, że firma przestrzega zasad prywatności. Audyty IT mają na celu sprawdzenie, czy system informatyczny firmy skutecznie chroni jej majątek, transakcje oraz procesy, zapewnia integralność danych i dostarcza właściwe informacje. Przeprowadzenie audytu pozwala także ocenić reakcję pracowników na sytuacje zagrażające cyberbezpieczeństwu, takie jak testy penetracyjne, czyli symulowane ataki, które pomagają wykryć luki w zabezpieczeniach. Ważne jest, aby zakres audytu był dostosowany do indywidualnych potrzeb i sytuacji firmy.

Jednocześnie pracownicy powinni być świadomi sposobu pozyskiwania danych, uprawnień do ich przetwarzania, lokalizacji przechowywania oraz zasad niszczenia danych. Polityka bezpieczeństwa obejmuje również sprzęt, taki jak laptopy czy tablety, i określa zasady jego aktualizacji, przechowywania oraz procedury zgłaszania utraty danych lub kradzieży (biznes.gov.pl, 2022).

Doświadczenia pokazują, że konieczne wydaje się szersze podejście do cyberbezpieczeństwa. Wskazuje się na konieczność zarządzania samym internetem w ujęciu ponadnarodowym (Uhma, 2017).

8. Jak przebiega cyberatak?

MITRE to amerykańska organizacja non-profit, która angażuje się m.in. w działania związane z cyberbezpieczeństwem. Zaproponowała ona szczegółową klasyfikację ataków cybernetycznych, mających na celu kradzież informacji z serwerów przedsiębiorstw, a także opisała przebieg typowego cyberataku (Stinet, 2020). Posiada on zazwyczaj następujące etapy:

Pierwszy etap to uzyskanie wstępnego dostępu. Przestępcy wykorzystują luki w zabezpieczeniach systemów firmowych lub stosują *phishing*, aby zdobyć dostęp do wewnętrznych sieci.

Drugim etapem jest rozpoczęcie działania przez cyberprzestępców. Po dostaniu się do sieci przestępcy mogą uruchomić złośliwe oprogramowanie, które pozwoli im na dalsze poszukiwanie luk w systemie.

Trzeci etap polega na utrzymaniu się w sieci. Przestępcy starają się uniknąć wykrycia i likwidacji swojego nieuprawnionego dostępu.

Czwarty etap to rozszerzenie uprawnień. Przestępcy dążą do zdobycia większych uprawnień, aby uzyskać dostęp do cennych materiałów do kradzieży.

Piąty etap to omijanie zabezpieczeń. Przestępcy stosują różne metody, aby uniknąć wykrycia przez systemy obronne, takie jak naśladowanie standardowych zachowań.

Szósty etap to uzyskanie uwierzytelnienia. Przestępcy manipulują kontami w celu zmiany uprawnień lub przechwytują ruch sieciowy, aby zdobyć ważne dane uwierzytelniające.

Siódmy etap to wyszukiwanie zasobów. Przestępcy przeszukują różne segmenty sieci, aby zlokalizować zasoby o największej wartości.

Ósmy etap to gromadzenie i kradzież danych. Przestępcy przesyłają skradzione dane z chronionych sektorów do innych miejsc i usuwają je z systemu.

Dziewiąty etap to zarządzanie i kontrola. Po wykradzeniu danych, przestępcy usuwają ślady, aby uniknąć wykrycia.

MITRE przygotowała tę klasyfikację, aby organizacje miały świadomość zagrożenia i mogły wdrożyć odpowiednie zabezpieczenia, minimalizując ryzyko cyberataków. Poznanie sposobów działania przeciwnika jest kluczowe dla skutecznej ochrony (Kulik, 2023).

Oczywiście cyberatak nie musi przebiegać w taki właśnie sposób. Może to być dowolny wariant powyższego scenariusza z naciskiem na poszczególne jego etapy. Scenariusz ataku dla przedsiębiorstw może przybrać zgoła odmienną formę. Po pojawieniu się pierwszych symptomów ataku, które — jak wspomniano — często mogą

mieć charakter problemów technicznych, osoby odpowiedzialne za infrastrukturę informatyczną mogą podjąć drastyczne decyzje. Chodzi o wyłączenie w celach bezpieczeństwa wszystkich lub dużej części systemów komputerowych. Decydenci odpowiedzialni za infrastrukturę informatyczną, nie znając sposobu i celu ataku, mogą chcieć zminimalizować w ten sposób potencjalne straty. Powyższe działanie jest bardzo logiczne, co nie zmienia faktu, że wpływa ono na powstawanie kosztów, a przede wszystkim upośledza funkcjonowanie samej firmy. Właściwe należy stwierdzić, że podczas ataku często należy przyjąć podejście sytuacyjne zależne od pojawiających się działań cyberprzestępców, ale także wielkości przedsiębiorstwa, branży, w której działa, i wreszcie rodzaju i skali ataku. Stworzenie uniwersalnego sposobu postępowania w takiej sytuacji jest trudne, jeśli nie niemożliwe.

9. Firmy zagrożone atakami

W roku 2021 aż dwie trzecie firm doświadczyło cyberincydentu, znalazło się w sytuacji zagrażającej bezpieczeństwu danych i systemów IT. Zastanawiający jest fakt, że sami przedsiębiorcy oceniają swoją odporność na cyberataki jako niską. Cyberataki mogą być bardzo kosztowne dla firm, a całkowity koszt może być trudny do oszacowania, w zależności na przykład od wielkości i profilu przedsiębiorstwa, szczególnie gdy dochodzi do utraty danych, utraty zaufania partnerów biznesowych i osłabienia pozycji na rynku (biznes.gov.pl, 2023).

Wraz z dalszym rozwojem internetu należy spodziewać się wzrostu częstotliwości cyberataków. Duże znaczenie może mieć pojawienie się internetu rzeczy (IoT) — podłączenie do internetu zupełnie nowego rodzaju urządzeń przyniesie potencjalne zagrożenia i zarówno przedsiębiorstwa, jak i pojedyncze jednostki będą je musiały wziąć pod uwagę (Rot & Blaicke, 2016).

10. Zakończenie

Podsumowując, cyberbezpieczeństwo jest dziedziną, która zyskuje coraz większe znaczenie nie tylko w biznesie. Wraz z rozwojem technologii liczba cyberataków stale rośnie, a ich skala i złożoność zagrażają zarówno jednostkom, jak i organizacjom na różnych poziomach wielkości i złożoności. Zrozumienie i świadomość zagrożeń cybernetycznych są kluczowe dla utrzymania bezpieczeństwa struktury informatycznej, a tym samym danych i prywatności.

Współczesne cyberataki mają różnorodne cele, od kradzieży danych, poprzez sabotowanie działania systemów, aż po wyłudzanie okupów. Wszystkie te zagroże-

nia mogą poważnie wpłynąć na stabilność finansową i reputację firm, instytucji, a nawet rządów.

Przedsiębiorstwa stają w obliczu nieustannego wyzwania, jakim jest ochrona swoich, nie tylko cyfrowych aktywów, przed atakami. Przyjęcie odpowiednich strategii i rozwiązań w zakresie cyberbezpieczeństwa staje się nieodzowne dla przetrwania na konkurencyjnym rynku. Inwestycje w zabezpieczenia (takie jak firewalle, systemy wykrywania intruzów, szyfrowanie danych) czy regularne szkolenia pracowników to niezbędne kroki, które pomagają minimalizować ryzyko ataków i ograniczać potencjalne straty.

Ważne jest również, aby społeczeństwa i organizacje rozumiały, że koszty związane z cyberatakami nie ograniczają się jedynie do naprawy i odtworzenia uszkodzonych systemów, skutki cyberataku mogą być bowiem odczuwane przez długi czas. W związku z tym cyberbezpieczeństwo nie powinno być traktowane jako luksusowy dodatek, lecz jako nieodłączna część strategii każdej firmy czy organizacji. Zapobieganie cyberzagrożeniom i reagowanie na nie musi być priorytetem zarówno dla małych, średnich, jak i dużych przedsiębiorstw, ale także agencji rządowych czy innych organizacji. Dążenie do maksymalnego zabezpieczenia danych i systemów przed cyberatakami to nie tylko wymóg, ale również inwestycja w przyszłość. Jedynie poprzez odpowiednią edukację, skuteczne rozwiązania technologiczne oraz ciągłe doskonalenie procedur bezpieczeństwa można stawić czoła rosnącemu zagrożeniu cybernetycznemu i chronić swoje najcenniejsze zasoby.

Bibliografia

biznes.gov.pl. (2022, 9 września). *Cyberbezpieczeństwo w małej i średniej firmie*. https://www.biznes.gov.pl/pl/portal/004175 (2023.01.07).

CFO Insights. (2016, grudzień). *Ukryte koszty cyberataku: analiza skutków z perspektywy firmy*. https://www2.deloitte.com/pl/pl/pages/rozwiazania-dla-cfo/articles/cfo-insights/ukryte-koszty-cyberataku-analiza-skutkow-z-perspektywy-firmy.html (2023.01.07).

Klich, L., & Sochala, C. (2016). Bezpieczeństwo w cyberprzestrzeni jako wyzwanie dla współczesnych państw — zarys problemu. W: J. Zimny (red.), *Bezpieczeństwo. Rodzina — naród — społeczeństwo*. Wyższa Szkoła Ekonomiczna w Stalowej Woli, Katolicki Uniwersytet Lubelski.

Kulik, W. (2019, 16 marca). *Etapy cyberataku na firmę*. https://www.benchmark.pl/aktualnosci/etapy-cyberataku-na-firme.html

Michałkiewicz, P. (2016). Cyberprzestrzeń a bezpieczeństwo narodowe. *Kultura Bezpieczeństwa*, 5, 190.

PBSG. (2021, 27 sierpnia). *Typy cyberataków, które zagrażają bezpieczeństwu w firmach*. https://www.pbsg.pl/typy-cyberatakow/ (2023.01.07).

Polska Bezgotówkowa. (2022, 22 sierpnia). Cyberatak — co to i jak się przed nim bronić? https://polskabezgotowkowa.pl/akademiaprzedsiebiorcy/cyberatak-co-i-jak-sie-przed-nim-bronic

Rot, A., & Blaicke, B. (2016). Zagrożenia wynikające z implementacji koncepcji internetu rzeczy, rekomendacje dla organizacji i dostawców rozwiązań. *Informatyka Ekonomiczna. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, *3*(41), 76.

Stinet. (2020, 19 października). *Czym jest MITRE ATT&CK*. https://stinet.pl/czy-jest-mitre-attck/ (2023.01.07).

Uhma, P. (2017). Suwerenne, wielostronne czy międzyrządowe zarządzanie internetem jako globalnym dobrem wspólnym. *Państwo i Społeczeństwo*, *17*(3), 26–31.

Types and Characteristics of Cyberattacks and Basic Measures Regarding Cybersecurity

Abstract. With the growing use of advanced information technologies, cyberattacks targeting computer systems, servers, programmes, sensitive data, smartphones and computer networks are becoming increasingly common. Knowledge of the most typical forms of cyberattacks and methods of defending against them should be one of the key competences of modern employees. Since a typical cyberattack usually follows a predictable sequence of stages, properly trained employees are a key element of any cybersecurity system as they can be its greatest asset or its weakest link. Another aspect that employees should be aware of are the potential effects, including financial ones, of a typical cyberattack for an enterprise.

Keywords: cybersecurity, cyberattack, IT infrastructure, digitization