Nowoczesne Systemy Zarządzania
Zeszyt 16 (2021), nr 4 (październik-grudzień)
ISSN 1896-9380, s. 43-54
DOI: 10.37055/nsz/147080

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 16 (2021), No. 4 (October-December)
ISSN 1896-9380, pp. 43-54
DOI: 10.37055/nsz/147080

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Wpływ rozwoju cyberprzestępczości na funkcjonowanie współczesnych organizacji

The impact of cybercrime trends on the functioning of modern organizations

Damian Szafranek
Wojskowa Akademia Techniczna, Wydział Bezpieczeństwa, Logistyki i Zarządzania
damian.szafranek@student.wat.edu.pl; ORCID: 0000-0003-1990-5638

Abstrakt. Rozwój technologiczny stawia przed współczesnymi organizacjami niebywałe szanse, ale wiążą się z nimi poważne wyzwania. Cyberprzestępczość jest zagrożeniem mogącym dotknąć organizacje niezależnie od ich rozmiaru czy pozycji na rynku. Odpowiednie zrozumienie aktualnych zagrożeń spowodowanych cybernetycznymi oraz funkcjonowania mechanizmów pozwalających minimalizować ich skuteczność jest kluczowe z perspektywy współczesnych organizacji. Celem pracy jest określenie aktualnych zagrożeń wynikających z rozwoju cyberprzestępczości oraz metod ich zapobiegania w kontekście funkcjonowania współczesnych organizacji. Główny problem badawczy pracy został zdefiniowany w formie pytania: Jaki wpływ wywiera rozwój cyberprzestępczości na funkcjonowanie współczesnych organizacji? W pracy wykorzystano następujące metody badawcze: metodę dedukcji oraz metodę analizy statystycznej – które pozwoliły na właściwą interpretację istniejących danych, wnioskowanie i syntezę – co pozwoliło odpowiedzieć na postawione pytanie badawcze. Wykorzystano również analizę źródeł (głównie monografii i artykułów naukowych) dotyczących badanego tematu.
Słowa kluczowe: cyberbezpieczeństwo, organizacja, phishing, zagrożenia, Internet

Abstract. Technological developments present today's organizations with incredible opportunities, but they come with significant challenges. Cybercrime is a threat that can affect organizations regardless of their size or market position. A proper understanding of the current threats of cyber attacks and the functioning of mechanisms to minimize their effectiveness is crucial from the perspective of modern organizations. The aim of the study is to identify current threats resulting from the development of cybercrime and methods of their prevention in the context of the functioning of modern organizations. The main research problem of the paper was defined in the form of a question: What impact does the development of cybercrime have on the functioning of modern organizations? The following research methods were used in the research paper: deduction method and statistical analysis method which allowed for proper interpretation of existing data, inference and synthesis – which allowed for answering the research question considered in the paper. The analysis of sources (especially monographs and scientific articles) on the topic under study was also used.
Keywords: cyber security, organization, phishing, vulnerabilities, Internet

Wstęp

Rozwój społeczeństwa informacyjnego niesie za sobą wiele wyzwań dla funkcjonowania współczesnych organizacji. Stale zmieniające się zagrożenia wymagają ciągłego dostosowywania się oraz zwiększania standardów bezpieczeństwa. Celem pracy jest określenie aktualnych zagrożeń wynikających z rozwoju cyberprzestępczości oraz metod ich zapobiegania w kontekście funkcjonowania współczesnych organizacji. Realizacja celu pracy jest możliwa dzięki odpowiedniej analizie statystyk z zakresu cyberprzestępczości, gdyż jest to istotny wyznacznik aktualnych zagrożeń oraz stanowi element umożliwiający dedukcję rozwoju zagrożeń cyberprzestępczością w przyszłych latach. Określenie charakterystyki współczesnych zagrożeń stanowi pierwszy krok w przygotowaniu bezpiecznego środowiska funkcjonowania organizacji. Dzięki analizie dokumentów oraz literatury przedmiotu możliwe jest syntetyczne przedstawienie głównych metod minimalizujących skutki lub przeciwdziałające atakom cyberprzestępców. Świadomość konsekwencji, jakie niosą za sobą zagrożenia, cyberprzestępczości zmusza współczesne organizacje do ciągłego rozwoju oraz wprowadzania coraz to nowych mechanizmów oraz procesów wspierających zapewnienie bezpiecznego funkcjonowania w cyberprzestrzeni. Zrozumienie istoty i sposobu funkcjonowania zabezpieczeń w kontekście zagrożeń cyberbezpieczeństwa jest szczególnie istotnym czynnikiem mogącym definiować istnienie organizacji na współczesnym rynku.

Współczesne środowisko bezpieczeństwa

Wpływ rozwoju technologicznego na funkcjonowanie człowieka widoczny jest nie tylko w obszarach kulturowych, edukacji czy życiu społecznym, lecz również w funkcjonowaniu współczesnych organizacji. Rozwój społeczeństwa informacyjnego niesie za sobą wyzwania, których odpowiednie podjęcie stanowić może o tym, czy zostaną one uznane za zagrożenie, czy za szansę. Dzięki odpowiedniej reakcji oraz świadomości istniejących zagrożeń możemy odpowiednio zinterpretować zaistniałą sytuację oraz podjąć odpowiednie środki celem ochrony szczególnych podatności.

Odpowiednie zrozumienie współczesnych zagrożeń jest kluczowym elementem w budowaniu bezpieczeństwa organizacji. Analizując zagrożenia dla człowieka związane z rozwojem technologicznym, możemy wyróżnić sześć typów zagrożeń (Furmanek, 2014, s. 23-24):

- zagrożenia psychologiczne;
- zagrożenia o charakterze technicznym;
- zagrożenia o charakterze medycznym;
- zagrożenia o charakterze prawnym;
- zagrożenia o charakterze społecznym;
- zagrożenia informacyjne wynikające z rozwoju współczesności.

Wymienione zagrożenia stanowią zdecydowanie poważne problemy, z którymi zmierzyć musi się całe społeczeństwo, ale w zarówno bliskiej, jak i dalszej perspektywie największe zagrożenia w funkcjonowaniu organizacji są to zagrożenia techniczne.

Zrozumienie istoty oraz form, jakie przybierają współczesne zagrożenia techniczne, możliwe jest dzięki analizie obecnych trendów cyberprzestępczości (Sztaudyner, 2004, s. 127-129). Analiza ostatnich 10 lat działania cyberprzestępców pozwoli na wyróżnienie obszarów funkcjonowania organizacji, które w sposób szczególny narażone są na ataki.

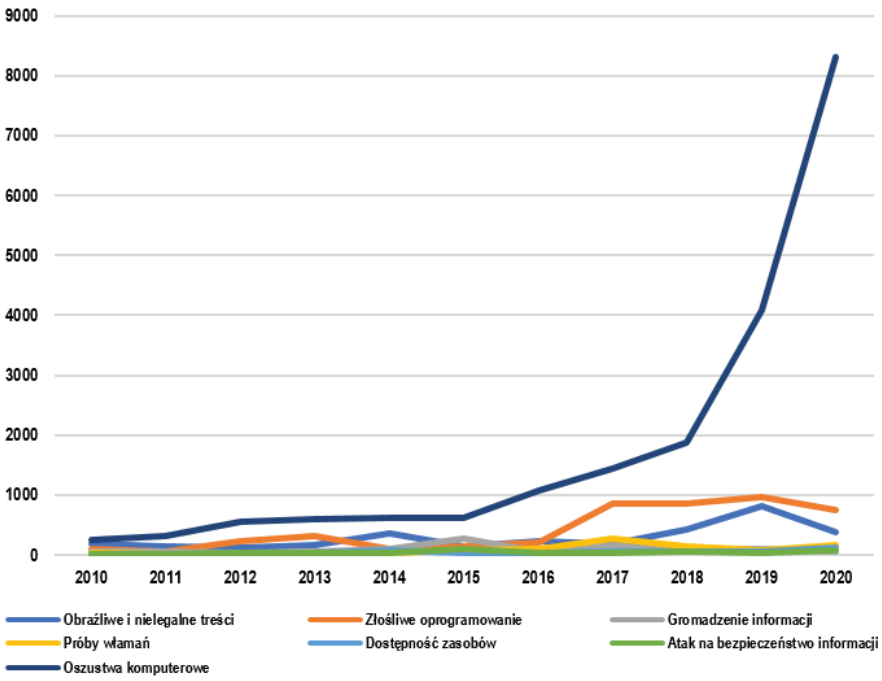
Przeprowadzenie dogłębnej analizy trendów w zakresie cyberprzestępczości możliwe jest dzięki działalności zespołu CERT działającego w strukturach NASK. Do zadań CERT Polska należą między innymi monitorowanie zagrożeń cyberbezpieczeństwa oraz incydentów na terenie krajowym (Smolski, 2015, s. 483-485). Efektem tych działań są coroczne raporty, które umożliwiają przeprowadzenie dokładnej analizy typów oraz natężenia zagrożeń w okresie 2010-2020 (zob. wykres 1).

Ogólna analiza zagrożeń widocznych na przestrzeni 10 lat pokazuje, iż niezależnie od typu incydentu widoczny jest pewien wzrost rejestrowanych incydentów. Jednym z istotnych czynników wpływającym na zwiększenie liczby zgłaszanych incydentów jest sam fakt zwiększania się liczby użytkowników Internetu, drugim natomiast jest świadomość możliwości zgłaszania incydentów. Na wykresie 1 jednak możemy zauważyć znaczący wzrost trzech typów incydentów, które w znacznym stopniu odróżniają się skalą występowania od pozostałych.

Pierwszym typem są oszustwa komputerowe, które w przeważającej części składają się z *phishingu*. Jako *phishing* należy rozumieć oszustwo, podczas którego przestępca podszywa się pod instytucję lub osobę celem uzyskania korzyści. Początkowo *phishing* rozumiany był jako metoda umożliwiająca uzyskanie poufnych informacji, współcześnie jednak pojęcie to ma znacznie szersze znacznie, a sam *phishing* może przybierać formy ograniczane jedynie przez kreatywność przestępcy (Lubowiecki, 2017, s. 30-31).

Kolejnym istotnym rodzajem zagrożenia jest złośliwe oprogramowanie. Na nie składają się programy komputerowe, dzięki którym cyberprzestępcy zyskują niemal całkowitą władzę nad naszym komputerem. Oprogramowania te mogą służyć zarówno do zbierania poufnych informacji, wykorzystywania zasobów sprzętowych naszego urządzenia między innymi do kopania kryptowalut, ale też do dalszego infekowania kolejnych urządzeń. Podobnie jak w przypadku *phishingu*, głównym ograniczeniem potencjalnych szkód w przypadku zainfekowania urządzenia jest kreatywność cyberprzestępcy, ale i jego umiejętności tworzenia oprogramowania.

Ostatnim typem incydentu wyróżniającym się pod względem występowania są obraźliwe i nielegalne treści. Elementami składowymi tego typu incydentu jest między innymi pornografia dziecięca, dyskredytacja, obrażanie, ale i spam stanowiący jego główną część składową. Jako spam należy rozumieć masowe wysyłanie wiadomości elektronicznych do wielu odbiorców (Piesiur, Słaboń, 2006, s. 286).



Wykres 1. Incydenty obsłużone przez CERT Polska w latach 2010-2020
Źródło: opracowanie na podstawie raportów rocznych CERT (CERT, 2020)

Wymienione powyżej typy incydentów oraz ich główne elementy składowe są ze sobą silnie powiązane, a ich wzmożone występowanie nie jest przypadkowe. *Phishing* rozumiany jako próba pozyskania informacji realizowany może być nie tylko dzięki szeroko rozumianej socjotechnice, lecz i przy wykorzystaniu złośliwego oprogramowania, którego zainstalowanie odbywa się właśnie dzięki odpowiedniej manipulacji ze strony cyberprzestępcy (Kowalczyk, 2014, s. 285). Zwiększenie skali potencjalnych ofiar może odbywać się przez zmasowane wysyłanie wiadomości będących spamem (Krakowiak, Bajor, 2018, s. 583-585). Masowa charakterystyka takich ataków mimo większego grona odbiorców często charakteryzuje się stosunkowo małą skutecznością w porównaniu do spersonalizowanych ataków. W literaturze przedmiotu jednymi z najpopularniejszych ataków wykorzystywanych przez cyberprzestępców są (Maciejowski, 2004, s. 35-38):

- włamania do sieci wewnętrznej Intranet;
- *phishing*;
- ataki na serwery, np. DDOS;
- kradzieże tożsamości;
- SPAM;
- ataki szkodliwego oprogramowania.

Widocznym jest, iż cyberprzestępcy, przeprowadzając ataki, kierują się głównie wizją szybkiego zarobku, co zwiększa prawdopodobieństwo przeprowadzenia ataku na organizację aniżeli na osobę fizyczną.

Współcześni cyberprzestępcy coraz częściej korzystają z innych metod, które w znacznym stopniu mogą podnosić skuteczność ataków przez nadanie pewnej autentyczności *phishingowi*. Jedną z wielu takich metod jest *spoofing* polegający na podszyciu się pod adresata wiadomości czy nawet numeru telefonu, powodując tym samym, iż ofiara może być przekonana, że osoba, z którą się kontaktuje, jest kimś zupełnie innym. Metoda ta umożliwia cyberprzestępcy zadzwonienie do nas z numeru telefonu, który będzie wyświetlał się na naszym urządzeniu jako numer infolinii naszego banku czy członka rodziny, choć nim nie jest (Chaładyniak, 2015, s. 41).

Rozwój technologiczny umożliwia również wykorzystywanie technologii sztucznej inteligencji do naśladowania między innymi głosu dowolnej osoby przez użycie technologii *deepfake* (Wasiuta, Wasiuta, 2019, s. 20-24). Dowolne łączenie tych metod wspierających *phishing* prowadzić może do drastycznego wzrostu jego skuteczności. Mimo iż współcześnie utworzenie przekonującego materiału *deepfake* wymaga wiele czasu oraz doświadczenia, czyniąc tę technologię niedostępną dla wielu cyberprzestępców, to jej potencjał oraz rozwój technologiczny może odmienić tę sytuację w krótkim czasie.

Cyberbezpieczeństwo w organizacji

Pracownicy stanowią kluczową rolę w funkcjonowaniu organizacji, ich zaangażowanie w pracę, odpowiednia organizacja oraz umiejętności stanowią podstawę jej funkcjonowania. Organizacja jednak jest równie silna co jej najsłabszy element, oznacza to, że pracownik będący podatnym na ataki cyberprzestępców jest zagrożeniem dla całej organizacji.

Pracownika możemy uznać za świadomego zagrożeń oraz ich ewentualnego wpływu na funkcjonowanie organizacji wówczas, gdy potrafi on wykorzystywać narzędzia pracy oraz rozpoznawać ewentualne zagrożenia. Możemy wyróżnić trzy podstawowe etapy składające się na skuteczność obrony pracownika przed zagrożeniami ze strony cyberprzestępców. Etapy te wymagają od pracownika odpowiedniego poziomu świadomości pozwalającego na podjęcie adekwatnych reakcji. Do etapów tych możemy zaliczyć: postępowanie, wykrywanie oraz reagowanie.

Przez postępowanie należy rozumieć umiejętność codziennego korzystania z urządzeń mających dostęp do Internetu. Służbowy telefon czy komputer stanowią narzędzia pracy, a więc pracownik powinien dokładnie wiedzieć, jak może z nich korzystać. Pracownik niewykorzystujący komputera stanowiącego narzędzie pracy do celów prywatnych w dużej mierze może ograniczyć możliwość wystąpienia incydentu. Umiejętność poprawnego wykorzystywania urządzeń w organizacji nie eliminuje możliwości wystąpienia zagrożenia, lecz może je znacznie ograniczyć.

Wykrywanie ewentualnych zagrożeń stanowi podstawę ich zwalczania, dzięki odpowiedniemu rozpoznaniu zagrożenia możemy podejmować kolejne kroki celem zwiększenia poziomu bezpieczeństwa. Odpowiednio wczesne wykrycie kampanii *phishingowej* udającej e-mail od działu księgowości czy ważnego klienta może udaremnić potencjalnie katastroficzny w skutkach atak.

Ostatnim, ale równie ważnym elementem świadomości pracowników jest reagowanie na zagrożenia. Wspomniany atak *phishingowy* mimo błyskawicznego wykrycia przez większość pracowników naszej organizacji ciągle może nieść za sobą poważne skutki. Odpowiednie zgłoszenie wykrytego przez pracownika zagrożenia pozwala na szybką reakcję minimalizującą atak.

Jedynie odpowiednie funkcjonowanie powyższych etapów może umożliwić minimalizowanie zagrożeń oraz podnoszenie bezpieczeństwa w organizacji. Każdy z wymienionych etapów wymaga jednak inwestycji poprzez ciągłe szkolenie pracowników celem podnoszenia ich kompetencji.

Budowanie świadomości może wydawać się inwestycją niemającą najwyższego priorytetu względem innych potrzeb organizacji, ale ewentualne straty spowodowane atakiem, którego można było uniknąć, mogą zmienić postrzeganie tychże priorytetów. Potencjalne konsekwencje wynikające z wystąpienia incydentu to między innymi:

- kradzież danych pracowników;
- kradzież danych klientów;
- podsłuch teleinformatyczny;
- zniszczenie danych;
- zmiana danych;
- sabotaż komputerowy;
- ingerencja w oprogramowanie;
- szkody wizerunkowe.

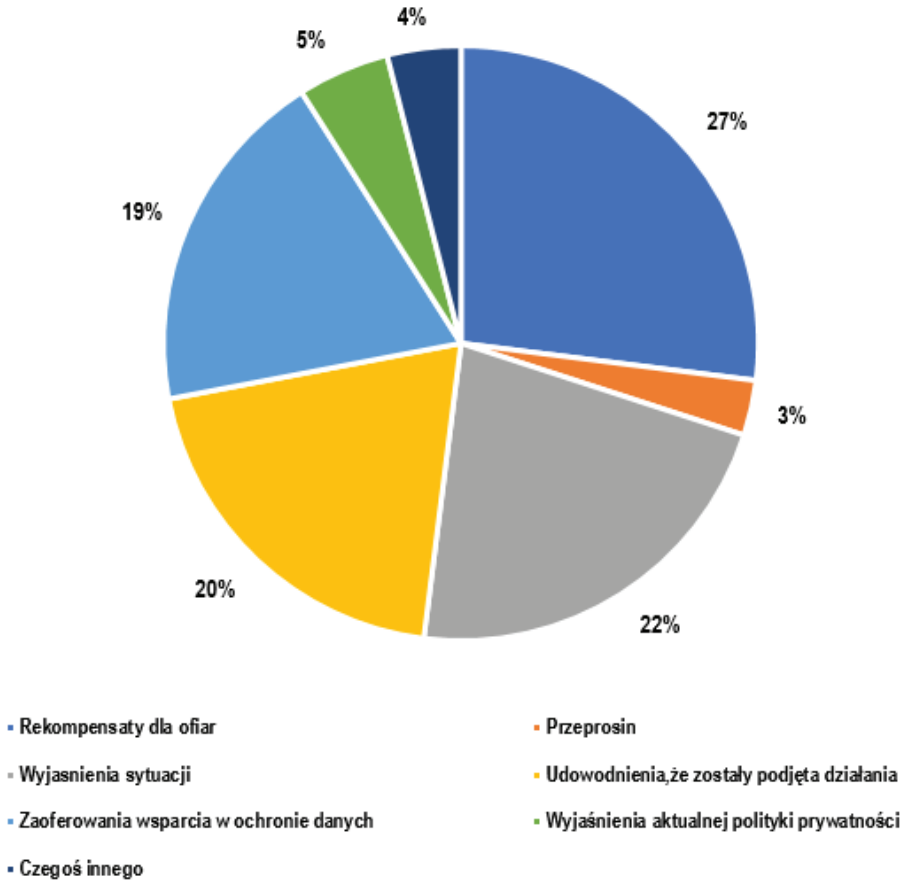
Incydenty z zakresu cyberbezpieczeństwa, podczas których miało miejsce ujawnienie danych osobowych klientów, niosą za sobą kary finansowe. Ich proporcjonalność zależy od skali wycieku. Jednym z największych incydentów ostatnich lat niosących za sobą poważne konsekwencje finansowe jest wyciek danych klientów sklepu internetowego morele.net z roku 2019. Kara finansowa nałożona przez UODO wynosiła 2,8 mln zł, czyniąc ją najwyższą ówczesną karą związaną z wyciekiem danych osobowych (Błachut, Dudzik, 2021, s. 29).

Ewentualny sabotaż komputerowy czy podsłuch teleinformatyczny mogą wpływać nie tylko na bezpośrednią skalę ewentualnego incydentu, lecz mogą być również powiązane z wywiadem gospodarczym, który w dłuższej perspektywie czasowej może definiować istnienie organizacji na rynku.

Powyższe zagrożenia oraz ich ewentualne konsekwencje mają istotną cechę wspólną. Odpowiednia świadomość pracowników w zakresie postępowania, wykrywania oraz reagowania na nie może w znaczącym stopniu zminimalizować ich

występowanie. Całkowita eliminacja zagrożenia wydaje się niemożliwa, ale ewentualne koszty związane ze szkoleniem pracowników w perspektywie konsekwencji wystąpienia zagrożenia wydają się znikome.

Kary finansowe nie są jednak jedynymi konsekwencjami wystąpienia incydentu. Klienci, których dane zostały ujawnione, zmieniają postrzeganie organizacji. Potencjalne zagrożenia powstałe w wyniku działalności cyberprzestępców mogą w istotnym stopniu wpływać na funkcjonowanie organizacji. Całkowita eliminacja tychże zagrożeń wydaje się nieosiągalnym wyzwaniem. Błąd ludzki czy też podatności oprogramowania powodują, iż proces budowania cyberbezpieczeństwa w organizacji ma charakter ciągły. Wystąpienie incydentu niesie za sobą również konsekwencje w postrzeganiu organizacji przez klientów.



Wykres 1. Oczekiwania klientów wobec wystąpienia incydentu z zakresu ochrony danych osobowych
Źródło: PwC US, *Protect.me Survey*, 2017

Analizując wykres 2, obrazujący oczekiwania klientów w kwestii reakcji organizacji na wystąpienie incydentu, można zauważyć, iż opinie wydają się być podzielone. Podjęcie reakcji służącej odbudowaniu zaufania jest niezwykle skomplikowanym wyzwaniem, na które nie ma prostej odpowiedzi. Wyjaśnienie klientom genezy zaistniałej sytuacji oraz przedstawienie realnych działań mających na celu zwiększenie zabezpieczeń jest jedynie początkiem działań zgodnie z oczekiwaniami klientów. Oprócz komunikacji na linii organizacja – klient ważne jest również zapewnienie wsparcia w zakresie ochrony danych, które zostały ujawnione wskutek wystąpienia incydentu. Najliczniejsze grono klientów oczekuje jednak pewnej formy rekompensaty za poniesione straty. Koszty finansowe wystąpienia incydentu składają się więc z wielu elementów, których suma może doprowadzić organizację do upadku. Odpowiednie zminimalizowanie prawdopodobieństwa wystąpienia zagrożenia dzięki wdrożeniu mechanizmów podnoszenia świadomości wydaje się najmniej kosztownym oraz najbardziej odpowiedzialnym zachowaniem.

Metody ochrony organizacji

Budowanie świadomości pracowników musi odbywać się przez odpowiednie szkolenia z zakresu postępowania, wykrywania oraz reagowania na zagrożenia. Dzięki odpowiedniemu zrozumieniu, jakie mechanizmy stoją za zagrożeniami, możliwe jest podejmowanie odpowiednich decyzji.

Edukacja pracowników w formie szkoleń stanowi istotną podstawę budowania ich świadomości w kwestii cyberbezpieczeństwa. Koniecznym jest, aby pracownicy rozumieli nie tylko zagrożenia, lecz również zabezpieczenia i procedury, których przestrzeganie niezbędne jest w zapewnianiu bezpieczeństwa. Zrozumienie istoty oraz funkcjonowania zabezpieczeń jest niezwykle ważne, ale równie istotnym jest ich poprawne użycie. Szkolenia poruszające te trzy kluczowe aspekty mogą budować świadomość pracownika, ale niezbędnym jest, aby odbywały się one cyklicznie, gdyż metody działalności cyberprzestępców ulegają ciągłej przemianie i doskonaleniu.

Pracownicy posiadający wiedzę teoretyczną z zakresu postępowania, wykrywania i reagowania powinni być poddawani regularnym testom praktycznym. Przeprowadzanie działań mających na celu zlokalizowanie słabych punktów w organizacji oraz sprawdzanie reakcji pozwala na ciągłe doskonalenie, którego wymaga środowisko.

Ostatnim kluczowym elementem w budowaniu i rozwijaniu świadomości pracowników organizacji jest stałe informowanie o nowych zagrożeniach. Świadomość aktualnych zagrożeń znacznie ułatwia ich spostrzeżenie oraz szybką i adekwatną reakcję. Budowanie świadomości pracowników jest procesem wymagającym ciągłego sprawdzania oraz przekazywania nowych informacji z zakresu rozwijających się zagrożeń.

Budowanie świadomości pracowników nie jest jednak jedynym elementem mającym istotny wpływ na bezpieczeństwo organizacji. Odpowiednie metody oraz dobre praktyki stosowane przez pracowników w połączeniu ze zrozumieniem istniejących zagrożeń w sposób zasadniczy minimalizują ewentualne incydenty. Do szczególnie istotnych elementów podnoszących poziom bezpieczeństwa organizacji w cyberprzestrzeni zaliczamy:

- szyfrowanie danych;
- kopie zapasowe danych;
- odpowiednią politykę haseł;
- weryfikację dwuetapową.

Szyfrowanie danych jest to jedna z podstawowych metod ochrony danych. Uniemożliwienie odczytania danych przez osoby nieuprawnione pozwala na pewną formę ochrony w wypadku błędu ludzkiego. Należy jednak mieć na uwadze, iż szyfrowanie nośników czy załączników przesłanych mailowo jest równie ważne co szyfrowanie urządzeń mobilnych, takich jak telefony, tablety czy laptopy. Potencjalne zgubienie przez pracownika telefonu służbowego zawierającego korespondencję o szczególnej wartości dla organizacji stanowi poważne zagrożenie (Dotson, 2021, s. 48-50).

Kopie zapasowe danych nie stanowią bezpośredniej formy ochrony przed atakami cyberprzestępców, lecz mogą skutecznie zabezpieczyć organizacje przed atakiem typu *ransomware*. Regularne tworzenie kopii zapasowych może również zabezpieczyć organizacje na wypadek utraty dostępu do urządzenia w przypadku wszelkich sytuacji kryzysowych (Rot, Pękala, 2016, s. 96-98).

Odpowiednia polityka haseł jest podstawowym zabezpieczeniem, z jakim będzie miał kontakt pracownik oraz jaki może powstrzymać potencjalnych cyberprzestępców. Jako politykę haseł należy rozumieć nie tylko tworzenie odpowiednich haseł, lecz również ich przechowywanie. W przypadku braku weryfikacji dwuetapowej podczas tworzenia hasła niejako ustanawiamy tym samym poziom bezpieczeństwa dla organizacji. Podstawowe zasady dotyczące tworzenia bezpiecznego hasła wymagają, aby składało się ono przynajmniej z 8 znaków, posiadało dużą i małą literę, przynajmniej jedną cyfrę oraz znak specjalny. Biorąc pod uwagę, iż hasła powinny być używane jednorazowo oraz być trudne do odgadnięcia, powoduje to pewne problemy z ich zapamiętaniem. Zdecydowanym ułatwieniem w zarządzaniu licznymi hasłami jest menedżer haseł. Rozwiązanie to pozwala w bezpieczny sposób przechowywać oraz często generować hasła składające się nawet z 60 znaków. Baza danych, w której przechowywane są wszystkie dane dostępu, zabezpieczona jest wtedy jedynym hasłem, które pracownik powinien pamiętać. Rozwiązanie takie zdecydowanie ułatwia pracownikom używanie skomplikowanych haseł i nie przysparza problemów w codziennym użytkowaniu (Wiśniewski, 2018, s. 132-133).

Weryfikacja dwuetapowa stanowi wyjątkowy element ochrony organizacji przed ewentualnymi błędami pracowników czy atakami cyberprzestępców. Pracownik, logując się do poczty internetowej czy innych portali niezbędnych do pracy, musi

zazwyczaj podać nazwę użytkownika oraz hasło. Ewentualne uzyskanie tych danych przez cyberprzestępców mogłoby prowadzić do poważnego naruszenia bezpieczeństwa organizacji. Jedną z najskuteczniejszych metod ochrony przed tego typu incydentami jest właśnie weryfikacja dwuetapowa, która polega na dodatkowej metodzie autoryzacji logowania przez użytkownika (Reese i in., 2019, s. 359-360). Pięć najczęściej spotykanych metod weryfikacji dwuetapowej to:

- powiadomienia *pop-up*;
- kody przekazywane drogą wiadomości SMS;
- kody przekazywane drogą mailową;
- programowe tokeny;
- klucze U2F.

Większość z powyższych metod ma pewien punkt wspólny – nie chronią one użytkownika przed zagrożeniami, takimi jak *phishing,* w stu procentach. Zarówno powiadomienia *pop-up*, jak i kody autoryzujące przekazywane drogą mailową czy SMS-ową wraz z programowymi tokenami podatne są na ataki cyberprzestępców. Metody, takie jak *SIM-Swaping*, umożliwiające przejęcie wszelkich wiadomości przychodzących na dany numer telefonu czy też oprogramowanie szpiegujące na urządzeniu używanym do weryfikacji dwuetapowej zagraża bezpieczeństwu użytkownika (Awale, Gupta, 2019, s. 996). Szczególną spośród powyższych metod zapewniającą najwyższy poziom bezpieczeństwa, w szczególności przed atakami *phishingowymi*, jest klucz U2F. Zabezpieczenie to ze względu na konieczność fizycznego kontaktu z urządzeniem oraz brak możliwości pozyskania przechowywanych na nim informacji może w stu procentach uchronić przed atakami *phishingowymi*.

Budowanie świadomości pracowników zdecydowanie poprawia ogólny poziom bezpieczeństwa w organizacji. Dodatkowe zabezpieczenia w postaci zaszyfrowanych dysków czy weryfikacji dwuetapowej zdecydowanie mogą ograniczyć możliwości ataku cyberprzestępcy. Kolejnymi istotnymi czynnikami mogącymi mieć wpływ na wystąpienie ewentualnego incydentu jest dostęp pracowników.

Ograniczenie dostępu do informacji jest kluczowym elementem przyznawania uprawnień pracownikom. Każdy pracownik powinien posiadać dostęp do jedynie tych informacji, które są mu niezbędne do wykonywania czynności służbowych. Rozwiązanie to pozwala na ograniczenie strat podczas ataku cyberprzestępcy, ale i podczas ewentualnej próby sabotażu ze strony pracownika.

Ograniczenie dostępu fizycznego jest niejako dopełnieniem ograniczenia dostępu do informacji. Zabezpieczenia te mają na celu zapewnienie, że pracownik nie będzie w stanie dostać się do pomieszczeń, w których znajdują się urządzenia, nośniki oraz inne części wyposażenia technicznego organizacji, które nie są mu niezbędne do wykonywania czynności służbowych.

Podsumowanie

Rozwój zagrożeń wymaga ciągłego dostosowywania się przez współczesne organizacje. Stałe zwiększanie świadomości pracowników stanowi podstawowe zabezpieczenie, które umożliwia zminimalizowanie szans wystąpienia incydentu z zakresu cyberbezpieczeństwa. Wszelkie dodatkowe mechanizmy umożliwiające ochronę danych czy wprowadzające konieczność dwuskładnikowej weryfikacji są jedynie elementem wspomagającym i minimalizującym ewentualne błędy najważniejszego elementu każdej organizacji, jakim jest pracownik. Koniecznym jest więc wprowadzanie coraz to nowych zabezpieczeń, których odpowiednie funkcjonowanie gwarantować może tylko odpowiednio przeszkolony i świadomy pracownik. Stałe zwiększanie świadomości pracowników przez szkolenia oraz informowanie ich o aktualnych zagrożeniach stanowi podstawę w budowaniu cyberbezpieczeństwa współczesnej organizacji. Odpowiednio wyedukowany pracownik jest w stanie znacznie zwiększyć szanse organizacji na uniknięcie ataku, ale konieczna jest ciągła aktualizacja wiedzy o nowe zagrożenia. Rozwój oraz charakterystyka metod działania cyberprzestępców może zmieniać swoją specyfikę, wymagając tym samym od organizacji ciągłej analizy bieżącej sytuacji i reagowania na nią w krótkim czasie. Zwiększanie nakładów finansowych związanych z cyberbezpieczeństwem stanowi dla współczesnych organizacji inwestycję w przyszłość i jest niezbędne ze względu na stale zwiększającą się liczbę ataków.

BIBLIOGRAFIA

[1] Awale, S., Gupta P., 2019. Awareness of Sim Swap Attack, *International Journal of Trend in Scientific Research and Development (IJTSRD)*, nr 3(4).

[2] Błachut, J., Dudzik, S., 2021. Naruszenie ochrony danych osobowych. Problematyka prawna, *Przegląd Konstytucyjny*, nr 3.

[3] Chaładyniak, D., 2015. Wybrane zagadnienia bezpieczeństwa danych w sieciach komputerowych, *Zeszyty Naukowe WWSI*, nr 13(9).

[4] Dotson, C., 2021. Zarządzanie zasobami danych i ich ochroną, *Napędy i Sterowanie*, nr 4.

[5] Furmanek, W., 2014. Zagrożenia wynikające z rozwoju technologii informacyjnych, *Dydaktyka Informatyki*, nr 9.

[6] Kowalczyk, M., 2014. Zagrożenia systemów informatycznych e-administracji – szkodliwe oprogramowanie i ataki, *Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach*, nr 101.

[7] Krakowiak, M., Bajor, T., 2018. Współczesne zagrożenia związane z użytkowaniem sieci, *Prace Naukowe Akademii im. Jana Długosza w Częstochowie*, nr 6.

[8] Lubowiecki, D., 2017. Prawno-kryminalistyczna problematyka phishingu, ze szczególnym uwzględnieniem środowiska bankowości internetowej, *Kwartalnik Prawo–Społeczeństwo–Ekonomia*, nr 1.

[9] Maciejowski, T., 2004. *Firma w Internecie. Budowanie przewagi konkurencyjnej*, Kraków: Oficyna Ekonomiczna.

[10] Piesiur, T., Słaboń, M., 2006. *Ochrona adresu e-mail w Internecie przed spamem*, [w:] *Systemy wspomagania organizacji*, Katowice: Wydawnictwo Akademii Ekonomicznej.

[11] Reese, K. i in., 2019. A Usability Study of Five Two-Factor Authentication Methods, *Usable Privacy and Security*, nr 15.

[12] Rot, A., Pękala, M., 2016. Tworzenie kopii zapasowych i odzyskiwanie danych jako element systemu zarządzania ciągłością działania, *Informatyka Ekonomiczna*, nr 2(40).

[13] Smolski, W., 2015. *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, [w:] Marszał, M. (red.), *Rodzinna Europa*, Wrocław: Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[14] Sztaudyner, J., 2004. Wpływ przestępczości na zrównoważony rozwój, *Prakseologia*, nr 144.

[15] Wasiuta, O., Wasiuta, S., 2019. Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość, *Studia de Securitate*, nr 9(3).

[16] Wiśniewski, P., 2018. Systemy zarządzania bezpieczeństwem informacji w przedsiębiorstwie, *Zarządzanie*, nr 2.

NETOGRAFIA

[1] PwC US, *Protect.me Survey*, 2017. https://www.pwc.es/es/digital/soluciones-seguridad-negocio/assets/02_consumer.pdf (01.12.2021).

[2] CERT, 2020. *Raport roczny z działalności CERT Polska: Krajobraz bezpieczeństwa polskiego Internetu 2020*. https://cert.pl/uploads/docs/Raport_CP_2020.pdf (01.12.2021).