BEZPIECZEŃSTWO • 2018 nr 4
TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264

Daniel Gach
doktor, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Kształtowanie elementów kultury organizacyjnej zorientowanych na zachowanie bezpieczeństwa informacyjnego

Wprowadzenie

Każda organizacja jest złożonym systemem, którego przetrwanie oraz rozwój uzależnione są od wielu wewnętrznych i zewnętrznych czynników. Te determinanty mogą mieć różnorodny charakter, rozmaitą siłę oddziaływania i zasięg, odmienne jest również ich pochodzenie, ale jest pewną oczywistością, że członkowie organizacji, a szczególnie przedstawiciele ich władz, dążą do zapanowania nad nimi i ukierunkowania ich oddziaływania zgodnie ze swoimi intencjami. Zbiór tych działań możemy zatem podzielić ogólnie na instrumenty techniczne (technologiczne), związane z funkcjonowaniem maszyn, urządzeń i technologii, oraz te, które wynikają z czynności podejmowanych przez ludzi. Uogólniając, można stwierdzić, że ludzie w jednakowy sposób traktują materialne i niematerialne efekty swojej działalności, a we współczesnej gospodarce, w której globalna hiperkonkurencja przejawia się również brakiem przestrzegania praw własności intelektualnej, co w konsekwencji przejawia się m.in. plagiatowaniem rozwiązań, problemem jest zarówno wprowadzenie na rynek innowacyjnych produktów, jak i zabezpieczenie się przed utratą kluczowych informacji i wiedzy związanych z tym procesem. W związku z tym potrzeba ochrony informacji i zarządzania bezpieczeństwem systemów informatycznych w organizacjach osiągnęła poziom krytyczny.

Elementy bezpieczeństwa informacyjnego

Funkcjonując w ramach społeczeństwa informacyjnego w gospodarce opartej na wiedzy, wszystkie podmioty rynkowe powszechnie wykorzystują zasoby informacyjne zarówno te, które zaliczyć można do „miękkich", czyli dane, informacje i oprogramowanie, oraz osprzęt (zasoby „twarde"), tj. komputery, urządzenia peryferyjne i sieciowe. Ich działanie oraz sposób wykorzystania przez użytkowników mogą wywołać wiele różnorodnych skutków, w tym, niestety, również te negatywne dla samej organizacji, stając się dla niej źródłem zagrożeń. W związku z dynamicznym rozwojem technologii teleinformatycznej pojawiają się nowe, nieznane wcześniej sytuacje o nieprzewidywalnych póki co skutkach, stąd też specjaliści z tej dziedziny muszą nie tylko uczyć się, jak radzić sobie w tych nowych warunkach, ale również podejmować próby przewidywania trudności i przygotowywać się na ich hipotetyczne zaistnienie. Jest to szczególnie ważne dla zapewnienia odpowiedniego bezpieczeństwa informacyjnego. Wdrożenie rozwiązań technicznych z tego zakresu nie jest jednak wystarczające. Skuteczność procedur zapewniających bezpieczeństwo informacji zależy od kompetencji i niezawodności osób, które je wdrażają i używają. Mogą istnieć odpowiednie zabezpieczenia, ale jeśli menadżerowie nie zarządzają nimi skutecznie lub jeśli użytkownicy nie wiedzą, jak prawidłowo obsługiwać owe rozwiązania, to w takiej sytuacji element ludzki staje się czynnikiem zależnym, a nie dominującym. W dowolnym momencie użytkownicy wchodzą w interakcje z zasobami informacyjnymi organizacji poprzez różne urządzenia w określony sposób i z jakiegoś powodu. Te interakcje stanowią najsłabsze ogniwo w bezpieczeństwie informacji, a potwierdzeniem tej tezy są m.in. wyniki badań z początku pierwszej dekady XXI wieku, w ramach których stwierdzono, iż zachowania osób wewnątrz organizacji stanowią poważniejsze zagrożenie dla bezpieczeństwa informacji, niż działania podejmowane przez ludzi z jej otoczenia[1].

Firma konsultingowa Deloitte w swoim corocznym raporcie, zawierającym wyniki globalnych badań w zakresie zarządzania ryzykiem, wskazuje na dwa główne zidentyfikowane źródła ryzyka. Jednym z nich jest zagrożenie płynące z cyberprzestrzeni, które staje się coraz większym problemem, ponieważ liczba i wpływ naruszeń cyberbezpieczeństwa są coraz wyższe. Innym obszarem, który zwrócił baczną uwagę badaczy, jest potrzeba podjęcia przez instytucje proaktywnych działań w celu zachęcenia swoich pracowników do etycznych zachowań i stworzenia kultury organizacyjnej „świadomej ryzyka"[2]. Wskazuje się, że dzięki rozwojowi technologii i nowych form organizacji obserwowany jest postęp w zakresie zarządzania ryzykiem, ale też podkreśla się, że w nadchodzących latach proces ten prawdopodobnie stanie przed innymi, odmiennymi wyzwaniami. Dlatego też olbrzymie znaczenie ma odpowiednie przygotowanie ludzi do tych nowych sytuacji poprzez rozwój świadomości (percepcji) własnych zachowań i dostrzegania wszelkich możliwych ich konsekwencji oraz kształtowanie kompetencji właściwego reagowania na zagrożenia. Ze względu na fakt, że nie ma możliwości pełnego zdefiniowania charakteru i zakresu przyszłych zagrożeń,

---

1 A. Martins, J. Eloff, *Information Security Culture*, [w:] *Security in the Information Society. Visions and Perspectives*, eds. M.A. Ghonaimy, M.T. El-Hadidi, H.K. Aslan, Kluwer Academic Publishers, Boston 2002, s. 204.

2 *Global Risk Management Survey, 10th editions. Heightened Uncertainty Signals New Challenges Ahead*, Deloitte University Press 2018, s. 3.

istotnym jest, aby to poprzez kulturę kreować zachowania i postawy pracownicze mogące być punktem wyjścia w wypracowaniu właściwego sposobu reagowania na nowe niebezpieczeństwa.

Sposoby, w jakie ludzie wchodzą w interakcje z zasobami informacyjnymi, oraz to, jak zachowują się w środowisku pracy, z czasem stają się elementami pewnego większego schematu, według którego wykonywane są wszelkie czynności w organizacji. Wraz z upływem czasu ulega on utrwaleniu i staje się częścią kultury organizacyjnej. Ważne jest, aby w trakcie tego procesu ujawnić i ugruntować prawidłowe zachowania i postawy w kierunku bezpieczeństwa informacji, tak aby również i one stały się elementami kultury. Zachowanie pracowników wobec informacji musi być akceptowalne i powinno stać się częścią codziennego życia w przedsiębiorstwie. Przykładem takiego zachowania może być to, że informacje o kliencie muszą być traktowane z zachowaniem poufności lub że tylko autoryzowany personel może przeprowadzać naprawy i serwisować sprzęt komputerowy. W ten sposób możliwe jest wykreowanie kultury bezpieczeństwa informacji w organizacji.

W odniesieniu do ludzi zatrudnionych w organizacjach w ramach nauk o zarządzaniu formułowane są różne koncepcje i teorie, w których zarówno prezentuje się charakterystyczny sposób ich funkcjonowania, jak i wyjaśnia się powody określonych zachowań. Ich poznanie umożliwia i ułatwia odpowiednie oddziaływanie na pracowników, tak aby realizowali cele organizacji. Jednakże człowiek jest istotą złożoną oraz wielowymiarową i nigdy nie ma pewności, że będzie działał zgodnie z intencjami menadżerów. Dodatkowo ludzie uczą się i rozwijają, a nabyte umiejętności i zdolności mogą wykorzystywać w sposób diametralnie różny od pierwotnych założeń. Stąd też punktem wyjścia w podjętych rozważaniach jest prezentacja przykładowych zachowań pracowników, która umożliwi pełniejsze zrozumienie kwestii bezpieczeństwa informacyjnego w przedsiębiorstwach. Należy bowiem pamiętać, że zagrożenia utraty kluczowych, poufnych informacji mogą być spowodowane zarówno świadomym działaniem pracowników popełniających przestępstwa ze względu na zakładane indywidualne korzyści, jak również mogą być wywołane nieświadomym zachowaniem zatrudnionych osób, które nie dostrzegają niebezpieczeństwa lub naiwnie wierzą, że żaden zewnętrzny podmiot nie zechce wykorzystać ich otwartych działań.

Przykłady działań pracowniczych generujących zagrożenia dla bezpieczeństwa informacyjnego

Poniżej zaprezentowano przypadki działań pracowników, którzy, kierując się naczelną zasadą zaspakajania swoich potrzeb, nieświadomie, a nawet – naiwnie wierząc, iż nikt nie będzie chciał ich oszukać i okraść, podjęli działania narażające firmę na utratę poufnych, a zarazem kluczowych dla funkcjonowania organizacji informacji.

W roku 2013 w pewnej amerykańskiej firmie zajmującej się tworzeniem oprogramowania na zlecenie, kontrola bezpieczeństwa ujawniła, że jeden z jej wyróżniających się pracowników zlecał wykonywanie swoich codziennych zadań roboczych, na zasadzie podwykonawstwa, firmie konsultingowej z Chin (dziennikarze opisujący ten

przypadek nazwali te działania ironicznie „outsourcingiem pracy")[3]. Punktem wyjścia w odkryciu tego „nowatorskiego zachowania" był wniosek skierowany do firmy Verizon, operatora sieci telefonii komórkowej i dostawcy Internetu, o audyt bezpieczeństwa wykorzystywanych łączy internetowych w związku z podejrzeniem o naruszenie protokołów bezpieczeństwa. Władze firmy informatycznej kilka lat wcześniej podjęły decyzję o zwiększeniu zakresu wykorzystania telepracy i dlatego zezwoliły swoim programistom na pracę w domu w wybrane dni. Aby umożliwić bezpieczną realizację tego projektu, założony został standardowy koncentrator sieciowy VPN (*virtual private protocol*). Po dwóch latach użytkowania zaniepokojenie władz firmy wzbudziły pewne anomalie w jego funkcjonowaniu. Podczas audytu bezpieczeństwa odkryto istnienie otwartego i aktywnego przez kilka miesięcy połączenia VPN pomiędzy stacją roboczą jednego z pracowników, a niezidentyfikowanym komputerem z chińskiego miasta Shenyang. Początkowo podejrzewano, że Chińczycy wykorzystują złośliwe, szpiegujące oprogramowanie służące do wykradania poufnych informacji z firmy. Jednakże dzięki szczegółowej analizie przesyłanych w ramach tego połączenia dokumentów odkryto elektroniczne wersje faktur wystawianych dla pracownika firmy za prace wykonane przez chińską firmę konsultingową. Dodatkowo okazało się, że zatrudniony – użytkownik badanej stacji roboczej – prawie cały swój czas pracy poświęcał na przeglądanie portali społecznościowych, aukcji internetowych oraz gier sieciowych. Dowiedziono, że ów 40-letni, utalentowany i spokojny pracownik dobrowolnie udostępnił swoje bezpieczne łącze chińskiemu przedsiębiorstwu, którego pracownicy mieli odtąd bezpośrednio wykonywać powierzone mu zadania. Aby zapewnić pełne połączenie, wykorzystywany jako dodatkowe zabezpieczenie, uwierzytelniający połączenia token RSA został przesłany przesyłką kurierską do Chin. W ramach oficjalnego badania efektywności w firmie pracownik osiągał ponadprzeciętne wyniki, uzyskując tytuły pracownika miesiąca i związane z tym nagrody. Okazało się, że w podobny sposób w tym samym czasie działał w kilku innych przedsiębiorstwach, uzyskując rocznie dochody na poziomie kilkuset tysięcy dolarów i ponosząc koszty wynagradzania chińskiej firmy konsultingowej na poziomie około 50 tys. dolarów. Po wykryciu tego faktu pracownik został zwolniony z pracy.

W przypadku jednej z polskich firm informatycznych problemem okazały się postawy i zachowania pracownicze zwiększające prawdopodobieństwo wykradzenia poufnych informacji przedsiębiorstwa. Dwa lata wcześniej w firmie została podjęta decyzja o modernizacji przestrzeni biurowej w siedzibie ulokowanej we wspólnym centrum biznesowym. Zadanie to zostało powierzone Grupie Nowy Styl, która w ramach swojej oferty zarówno dostarcza meble biurowe, jak również, posiłkując się Działem Badań i Konsultingu Przestrzeni Pracy, przeprowadza kilkumiesięczne badania miejsc pracy, aby, wykorzystując koncepcję Activity – Based Working (ABW), zaproponować właściwe rozmieszczenie i wyposażenie poszczególnych stref pracy wyróżnionych w nowym projekcie[4]. Badania te obejmują m.in. analizę stylów pracy

[3] *US Employee 'Outsourced Job to China'*, „BBC News", 16.01.2013, https://www.bbc.com/news/technology-21043693 [dostęp: 20.09.2018].

[4] Opis przypadku został zrealizowany w oparciu o informacje uzyskane w trakcie badań własnych w Grupie Nowy Styl w latach 2017–2018 w ramach działalności statutowej Wydziału Zarządzania i Komunikacji Społecznej Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, zadanie badawcze nr: WZiKS/DS/8/2016.

rozpatrywanych działów, określenie siatki powiązań pomiędzy nimi, wyznaczenie poziomu wykorzystania przestrzeni oraz planowanej rezerwy dla przyszłych pracowników i nowych wdrożeń. Efektem końcowym jest projekt nowego biura zawierający propozycje stref aktywności i ich aranżacji. W rozpatrywanym przypadku firmy informatycznej główne problemy ujawnione w trakcie badań obejmowały niski poziom interakcji międzyludzkich oraz ograniczające bezpieczne funkcjonowanie niezbędne okablowanie biura, które, nieujęte w pierwotnym projekcie, wraz z rozwojem firmy osiągnęło wysoki poziom i musiało przebiegać wprost na podłodze poszczególnych pomieszczeń. Nowy, wdrożony projekt przestrzeni pracy zakładał rozmieszczenie stanowisk w formie „wewnętrznego kręgu", w którym pracownicy, siedząc przy biurkach ulokowanych obok siebie (pracując „ramię w ramię"), mieli monitory skierowane do wewnątrz pomieszczeń. Oczywiście wdrożono również elementy zabudowy ukrywające kable łączące poszczególne urządzenia. Jednakże po pewnym czasie pracownicy sami dokonali zmian, które zniweczyły efekt projektu. Biurka został rozsunięte i obrócone tak, że monitory skierowane były na zewnątrz pomieszczeń, w tym również w stronę okien, za którymi w niewielkiej odległości ulokowane były inne budynki. W ten sposób wykreowana została okazja do pozyskiwania poufnych informacji przez inne podmioty, a to dzięki obserwacji monitorów pracowników. Dodatkowo ponownie widoczne było okablowanie stanowisk pracy, które było nie tylko nieestetyczne, ale również stwarzało warunki zagrożenia dla zdrowia zatrudnionych osób poprzez wzrost ryzyka potknięć i upadków. Badacze z Grupy Nowy Styl przypuszczają, że powodem tych zmian było podejście pracowników firmy informatycznej do siebie nawzajem – bardziej zależało im na ukryciu przed współpracownikami nie tylko zakresu realizowanych obowiązków zawodowych, ale również innych form aktywności w Internecie (przeglądanych stron internetowych, portali społecznościowych i gier sieciowych) niż na zachowaniu odpowiednich standardów bezpieczeństwa informacyjnego.

Kultura organizacyjna i jej wpływ na pracowników

Od ponad dwudziestu lat wskazuje się, że kluczową grupą czynników decydujących o sukcesie organizacji są ich zasoby niematerialne, a wśród nich szczególne miejsce zajmuje kultura organizacyjna. Geert Hofstede mówi wprost o olbrzymim wpływie kultury na funkcjonowanie ludzi, stwierdzając, że jest ona „kolektywnym zaprogramowaniem umysłu, które odróżnia członków jednej grupy lub kategorii ludzi od drugiej" oraz „członków jednej organizacji od drugiej"[5]. Choć w tym przypadku słowo „zaprogramowanie" służy jako metafora, to jednak wskazuje, że zachowanie każdej osoby jest częściowo zdeterminowane jej wychowaniem oraz środowiskiem społecznym, w którym funkcjonuje. Powoduje to, że możliwe jest przewidywanie prawdopodobnych, zrozumiałych i typowych reakcji człowieka w normalnych warunkach jego funkcjonowania, a w szczególnych przypadkach również w sytuacjach odbiegających od standardowych. W czasie trwania swojego życia człowiek przyswaja określony

[5] G. Hofstede, *Kultury i organizacje. Zaprogramowanie umysłu*, przeł. M. Durska, Polskie Wydawnictwo Ekonomiczne, Warszawa 2000, s. 40 i 267.

wzorzec myślenia, odczuwania i zachowania, który cechuje się pewną stałością, ale można dokonywać jego zmiany. Jednakże wymaga to odpowiedniego czasu i podwójnego wysiłku. Po pierwsze, trudu rezygnacji z już przyswojonego wzorca i po drugie – powtórnej nauki nowych zachowań. Wiedza na temat tego procesu powinna być wykorzystywana przez organizacje, które podejmują decyzje o kształtowaniu pożądanych wzorców kulturowych u swoich pracowników.

Rozpatrując zagadnienia związane z wpływem kultury na zarządzanie zasobami ludzkimi, należy podkreślić, że wielu zajmujących się tą problematyką przedstawicieli świata nauki i praktyki wprost wskazuje, że wśród instrumentów i narzędzi oddziaływania na zasoby ludzkie w celu uzyskania zaangażowanych, twórczych i wykwalifikowanych pracowników znajdują się również techniki kulturowe[6]. Oznacza to, że kultura i jej elementy są wpisane w zakres zarządzania zasobami ludzkimi w każdym aspekcie funkcjonowania organizacji, w tym również w kreowaniu i rozwijaniu systemów bezpieczeństwa organizacyjnego. Edgar H. Schein stwierdza, iż wybierane oraz wdrażane w firmach strategie i praktyki zarządzania odzwierciedlają kulturowe założenia podstawowe, co oznacza, że również systemy motywacyjne i kontrolne w większości organizacji opierają się na założeniach dotyczących ludzkiej natury, a jeśli założenia te nie są podzielane przez menadżerów organizacji, wystąpią niespójne praktyki i fałsz[7].

W klasycznym już podziale elementów kultury dokonanym przez Scheina wyróżnia się trzy podstawowe poziomy i zarazem grupy elementów kultury: założenia podstawowe, normy i wartości oraz artefakty[8]. Choć wskazuje się na hierarchiczny układ tych elementów, w którym założenia podstawowe tworzą podstawę zaistnienia i rozwoju pozostałych, to należy zwrócić uwagę, że jakkolwiek w początkowym okresie tworzenia i kształtowania kultury ta prawidłowość jest oczywista, to w dalszym funkcjonowaniu zbiorowości będącej jej nośnikiem to oddziaływanie może mieć różnorodny przepływ i siłę (rysunek 1). Analogicznie możemy omawiać wpływ elementów kultury na zachowania i postawy członków określonej zbiorowości, choć w tym przypadku już od samego zaistnienia jednostki ludzkiej w obszarze oddziaływania danej kultury każdy z jej wymienionych poziomów może wpływać na człowieka z różną siłą i w odmienny sposób.

Uzupełnieniem poprzedniej koncepcji jest wskazywana przez Hofstedego kategoria bohaterów organizacyjnych. Są to osoby szczególnie znaczące dla danej instytucji, postacie z mitów organizacyjnych, istniejące historycznie lub współcześnie, utożsamiające pewne cechy, dzięki którym osiągnięty został indywidualny i zbiorowy sukces[9]. Są one następnie wyraźnie doceniane w danej kulturze organizacyjnej i tym samym traktowane jako pewien wzorzec zachowań. To również pewne wyobrażenia o idealnym typie pracownika, którego cechy, postawa i zachowania mają zagwarantować szybką karierę w firmie. Bohaterami organizacyjnymi mogą być również postacie fikcyjne, wymyślone np. dla celów marketingowych, ale dzięki odpowiedniej

---

6 T. Listwan, *Przedmiot, ewolucja i znaczenie zarządzania kadrami*, [w:] *Zarządzanie kadrami*, red. T. Listwan, Wydawnictwo C.H. Beck, Warszawa 2002, s. 6; A. Pocztowski, *Zarządzania zasobami ludzkimi*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2008, s. 32 i 34.

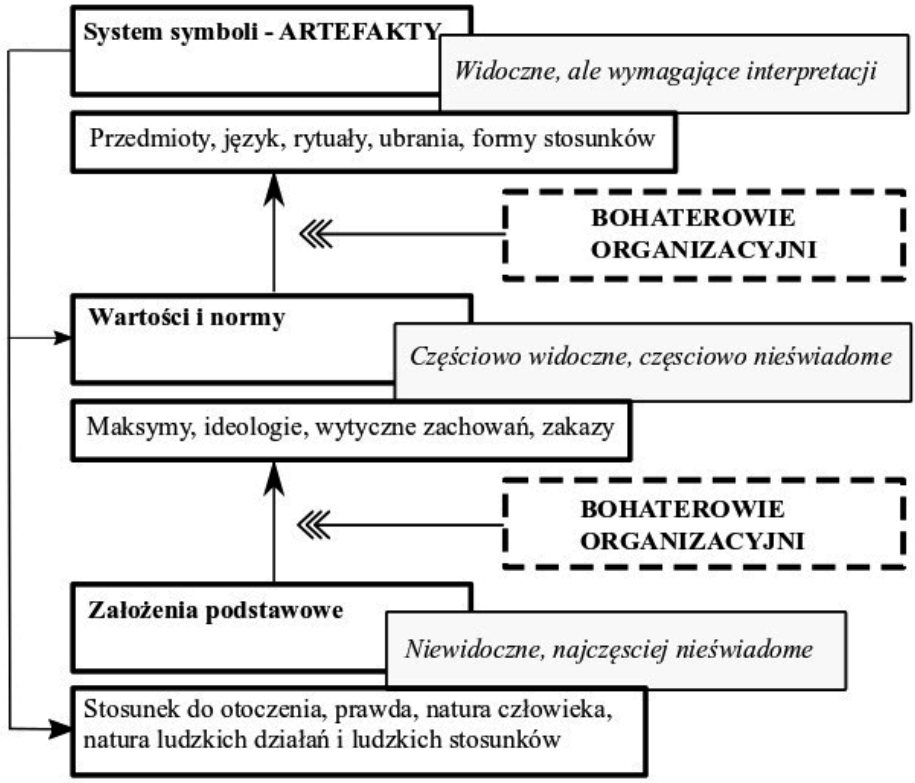
7 E.H. Schein, *Organizational Culture and Leadership*, Jossey-Bass A Wiley Imprint, San Francisco 2010, s. 145.

8 *Ibidem*, s. 22–30.

9 G. Hofstede, *op. cit.*, s. 43–44 i 274.

polityce funkcjonowania instytucji mogące stać się zbiorowym i jednocześnie akceptowanym wyobrażeniem pewnego wzorca działania jednostek.

Rysunek 1. Elementy kultury organizacyjnej w połączonym ujęciu Edgara H. Scheina i Geerta Hofstedego



Źródło: opracowanie własne na podstawie: G. Hofstede, *Kultury i organizacje*, przeł. M. Durska, Polskie Wydawnictwo Ekonomiczne, Warszawa 2000, s. 43–44; E.H. Schein, *Organizational Culture and Leadership*, Jossey-Bass A Wiley Imprint, San Francisco 2010, s. 23.

Jednakże należy zwrócić uwagę, że sama kultura może cechować się pewnym dualizmem, w jej ramach można wyróżniać wartości deklarowane i rzeczywiste. Podobna sytuacja ma miejsce w odniesieniu do bohaterów organizacyjnych: mogą to być oficjalnie prezentowane i przyjmowane jako wzorce postacie (np. założyciele firm: Henry Ford, Akio Morita – „Sony", Kiichirō Toyoda – „Toyota", Steve Jobs – „Apple"), ale również mogą to być ukryci bohaterowie, których sylwetki i dokonania prezentowane są w nieoficjalnych, często poufnych przekazach ustnych. Dodatkowo należy pamiętać, że pomiędzy postaciami z oficjalnej narracji, a tymi, które rzeczywiście traktowane są jako pożądane wzorce działania, mogą występować różnice. Takim historycznym przykładem może być propagandowa polityka z czasów PRL, w ramach której kreowano bohaterów organizacyjnych w osobach przodowników

pracy, a w rzeczywistości wśród pracowników powszechny był podziw dla „kombinatorów", potrafiących pozyskać dla zaspokojenia swoich indywidualnych potrzeb zasoby organizacyjne[10].

Bez względu na to, w jaki sposób zaistnieli bohaterowie organizacyjni i jak są postrzegani, ich wpływ na organizację jest znaczący. Jeżeli byli to założyciele firmy, to ich przekonania i system wartości w połączeniu z wybranymi założeniami określonej kultury narodowej stają się fundamentem założeń podstawowych kultury organizacyjnej, w tym tych odnoszących się do kwestii uczciwości, lojalności, staranności, a w konsekwencji – do bezpieczeństwa w organizacji.

Historia funkcjonowania wielu firm dostarcza argumentów potwierdzających stwierdzenie, że im energiczniej organizacja zapewnia o tym, jak ważne są dla niej pewne wartości, tym dotkliwiej pracownicy odczuwają rozdźwięk między głoszonymi ideami, a ich realizacją w praktyce[11]. Należy pamiętać, że w środowisku, w którym dostrzega się silne skupienie na wartościach, pracownicy są szczególnie uwrażliwieni na najmniejsze odejście od głoszonych zasad.

Kultura bezpieczeństwa

Kultura organizacyjna jest złożonym systemem, w ramach którego można wyróżnić szereg elementów składowych. Możliwe jest wyodrębnienie różnych subkultur związanych z poszczególnymi podsystemami organizacyjnymi lub opartymi na różniących się między sobą zbiorach treści (zawartości informacji). Subkultura jest podsystemem, który ma specyficzne wartości, normy i wiedzę, co wyróżnia ją w ramach ogólnej kultury korporacyjnej. Przykładowo: mogą to być wartości, normy i wiedza działu informatycznego lub działu sprzedaży, podczas gdy kultura bezpieczeństwa informacji jest subkulturą ze względu na treści i koncentruje się na społeczno-kulturalnych aspektach zarządzania bezpieczeństwem informacji[12]. Kai Roer definiuje kulturę bezpieczeństwa jako zbiór idei, zwyczajów i zachowań społecznych posiadanych przez daną społeczność lub grupę, wykorzystywanych przez nią, tak aby wytworzyć środowisko wolne od zagrożeń i niebezpieczeństw[13]. Kulturę bezpieczeństwa informacji można postrzegać również jako zestaw charakterystyk procedur realizowanych w przedsiębiorstwie, a związanych z zagwarantowaniem pewnych i bezpiecznych informacji, takich jak rzetelność i dostępność, które powinny być dostrzegane i realizowane przez organizację[14]. Ta kultura jest również zbiorem założeń o tym, co jest, a co nie jest dopuszczalne w organizacji w odniesieniu do bezpieczeństwa informacji.

Kultura korporacyjna pomaga budować niezbędne zaufanie pomiędzy różnymi partnerami organizacyjnymi, a wyróżniana w niej kultura bezpieczeństwa powinna

[10] Por.: *Współzawodnictwo pracy w życiu gospodarczym, społeczno-politycznym i propagandzie PRL*, red. B. Tracz, Drukpol, Katowice 2008.

[11] L. Bock, *Praca rządzi! Metody Google'a, które odmienią twoją pracę i życie*, Insignis Media, Kraków 2017, s. 391–393.

[12] T. Schlienger, S. Teufel, *Information Security Culture. The Socio-Cultural Dimension in Information Security Management*, [w:] *Security in the Information Society…*, *op. cit.*, s. 197–198.

[13] K. Roer, *Build a Security Culture*, IT Governance Publishing, Cambridgeshire 2015, s. 12.

[14] A. Martins, J. Eloff, *op. cit.*, s. 205.

wspierać wszystkie działania każdego pracownika. Jej kreowanie i rozwój jest odpowiedzią na syndrom „mój własny użytkownik jest moim największym wrogiem", będący wyrazem przekonania, że żadne wysoce rozwinięte systemy technicznych zabezpieczeń nie dają pełnej gwarancji bezpieczeństwa ze względu na duże prawdopodobieństwo popełnienia prostych błędów przez ich użytkowników, np. wykorzystywanie bardzo prostych haseł zabezpieczających czy też zapisywanie złożonych haseł – aby ich nie zapomnieć – w miejscach dostępnych również dla innych[15]. Kultura bezpieczeństwa informacyjnego poprzez wprowadzanie właściwych postaw i zachowań ma zmienić to przekonanie na przekaz, że pracownicy stają się zasobem sprzyjającym bezpieczeństwu. W odniesieniu do przytaczanej koncepcji elementów kultury organizacyjnej Scheina, w ramach kultury bezpieczeństwa wskazuje się przykładowe jej składniki:

- na poziomie artefaktów i rytuałów – tradycja corocznego uczestnictwa pracowników w kursach (szkoleniach) dotyczących bezpieczeństwa, praktyka cotygodniowej zmiany haseł;
- na poziomie wartości i norm – zasada bezwzględnego przestrzegania norm bezpieczeństwa przez wszystkich pracowników;
- na poziomie założeń podstawowych – dążenie do ugruntowania założenia, że pracownicy są organizacyjnymi „zasobami bezpieczeństwa".

Wyróżniane w ramach kultury bezpieczeństwa warstwy są otoczone bazowymi i zarazem zewnętrznymi podstawowymi uwarunkowaniami, a także normami społecznymi i wartościami, które, przykładowo, są wyrażone w prawie krajowym i międzynarodowym. Kultura bezpieczeństwa powinna określać trzy poziomy odpowiedzialności[16]:

- polityka korporacyjna;
- podsystem zarządzania;
- jednostki.

Na poziomie polityki korporacyjnej bezpieczeństwo informacji powinno być zdefiniowane jako cel organizacji. Oznacza to, że kierownictwo najwyższego szczebla jest odpowiedzialne za zdefiniowanie polityki bezpieczeństwa, w związku z czym muszą zostać zapewnione wystarczające zasoby do wdrożenia wyróżnionych w jej ramach działań. W większych organizacjach zadania związane z tym obszarem są realizowane przez specjalnie do tego celu powołane jednostki, na czele których stoi menadżer ds. bezpieczeństwa organizacji (*chief security officer* – CSO). W szczególnych przypadkach może to być osoba zarządzająca odpowiedzialna za bezpieczeństwo informatyczne (*chief information security officer* – CISO). Ich rola związana jest z identyfikowaniem, rozwijaniem, wdrażaniem i utrzymywaniem procesów bezpieczeństwa w całej organizacji w celu redukcji ryzyka, przygotowania właściwej odpowiedzi na incydenty, kreowania zachowań obronnych organizacji wobec nowych zagrożeń sektorowych i ograniczania narażenia na odpowiedzialność we wszystkich obszarach ryzyka finansowego, fizycznego i osobistego[17]. Działania te służą

[15] Por. A. Adams, M.A. Sasse, *Users Are Not the Enemy*, „Communiacations of the ACM" 1999, Vol. 42, No. 12, s. 40–46.

[16] T. Schlienger, S. Teufel, *op.cit.*, s. 198–199.

[17] Por. R. Cloutier, *Becoming a Global Chief Security Executive Officer. A How to Guide for Next Generation Security Leaders*, Butterworth-Heinemann, Oxford 2015.

m.in. ustanowieniu odpowiednich standardów i procedur kontroli ryzyka związanego z własnością intelektualną, ochroną danych osobowych, ochroną informacji niejawnych oraz wdrożeniu polityki oraz procedur związanych z bezpieczeństwem danych w systemach informatycznych. Jednostki bezpieczeństwa, w tym również bezpieczeństwa informacyjnego, wspierają władze organizacji w procesie rozwoju, wdrażania i zarządzania wizją, strategią i programem bezpieczeństwa organizacji. Jednakże należy pamiętać, że najwyższe kierownictwo w dalszym ciągu pozostaje odpowiedzialne za całość realizowanych czynności związanych z owymi procesami.

W ramach podsystemu zarządzania różni kierownicy działów są odpowiedzialni za zgodność polityki bezpieczeństwa informacyjnego i za jej wdrożenie w swoich jednostkach. Osoby te muszą być wystarczająco zaangażowane i zmotywowane do przestrzegania polityki bezpieczeństwa, ponieważ bez ich pomocy nie jest możliwe jej wdrożenie. To założenie wiąże się z przyjęciem odpowiednich wytycznych w procesie rekrutacji i selekcji nowo zatrudnionych pracowników – wskazuje się, aby wzbogacić wszystkie narzędzia rekrutacyjne o rozwiązania dające gwarancję odrzucenia osób nie wykazujących się takimi postawami i zachowaniami. Aby wdrażanie polityki bezpieczeństwa przebiegało sprawnie, zarząd musi zdefiniować oraz kontrolować różne instrumenty i narzędzia w jej ramach wykorzystywane. Ważne jest przygotowanie odpowiednich szkoleń dla kierowników i pracowników z szeroko pojmowanego bezpieczeństwa organizacyjnego. Należy również wprowadzić w ramach systemu ewaluacji i motywowania pracowników rozwiązania odkrywające zachowania zgodne z procedurami bezpieczeństwa i przyznawaniem za nie właściwych nagród, a wszelkie naruszenia bezpieczeństwa powinny być oceniane, nagłaśniane i ścigane. Ponadto strategia bezpieczeństwa musi być regularnie monitorowana i porównywana z wzorcami sektorowymi czy też branżowymi.

W odniesieniu do każdego pracownika dąży się do tego, aby wyrobić w nim skłonność do przyczyniania się do zachowania i wzrostu bezpieczeństwa organizacji. Wykorzystując odpowiednie rozwiązania w systemie rekrutacji lub poprzez dedykowane szkolenia, odkrywa się i rozwija w każdym z zatrudnionych krytyczne nastawienie. Kreowana jest sytuacja, w której pracownik ciągle poszukuje odpowiedzi na pytania:

- czy rozumie swoje zadanie?
- jakie są jego obowiązki?
- w jakich relacjach pozostają obowiązki wobec bezpieczeństwa informacji?
- czy pracownik dysponuje wystarczającą wiedzą, aby wypełnić swoje zadanie?
- czy potrzebuje pomocy?

Ważne jest, aby działał ostrożnie i z należytą starannością. Każde nieprawidłowe zachowanie ludzi lub systemów komputerowych (w tym wadliwe działanie) musi być rejestrowane i zgłaszane. Ponadto użytkownik musi zostać włączony do procesu analizy ryzyka, a firma powinna zainstalować system zgłaszania sugestii pracowników. Podsumowując, można uznać, że w odniesieniu do kultury bezpieczeństwa najważniejsze są:

- wzorowe, służące za przykład zachowania menedżerów;
- szkolenie pracowników w zakresie bezpieczeństwa, w tym inicjowanie i rozwijanie świadomości na temat ryzyka związanego z technologią informacyjną i szkolenia w zakresie korzystania z produktów zabezpieczających;
- nagradzanie zachowania zgodnego z zasadami bezpieczeństwa.

Ważne jest, by dostrzec, że zachowanie zgodne z zasadami bezpieczeństwa może również obejmować zgłaszanie naruszeń bezpieczeństwa. Informowanie kierownictwa o błędach i pomyłkach może pomóc organizacji poprawić zachowania związane z bezpieczeństwem poprzez lepsze zrozumienie możliwych zagrożeń i ryzyka.

Podsumowanie

Kultura niezwykle silnie determinuje ludzkie zachowania i postawy, co przejawia się m.in. niemożnością podjęcia działań niezgodnych z prawem, a polegających na wykradaniu istotnych informacji z firmy konkurencyjnej. Idealną sytuacją dla każdej organizacji byłoby posiadanie tak atrakcyjnej i silnej kultury, która byłaby w stanie wpływać na zachowania ludzi specjalnie zatrudniających się w danej firmie, aby przechwycić jej kluczowe, poufne informacje. W takich przypadkach pożądanym byłoby występowanie w kulturze organizacyjnej przedsiębiorstwa-ofiary takich elementów, które, oddziałując na potencjalnego przestępcę, mogłyby zmienić jego nastawienie na poziomie założeń podstawowych i przyczyniłyby się do uniemożliwienia mu dokonania czynu kradzieży własności intelektualnej.

Kształtowanie elementów kultury organizacyjnej zorientowanych na zachowanie bezpieczeństwa informacyjnego

Streszczenie

Współcześnie w zarządzaniu wskazuje się, że dominującymi, kluczowymi czynnikami sukcesu przedsiębiorstw są właściwie wykorzystane zasoby niematerialne, wśród których olbrzymią rolę odgrywa wiedza kreowana na bazie informacji, które z kolei są formowane na podstawie danych, przybierających postać olbrzymich zbiorów (tzw. *big data*). W ich pozyskiwaniu, gromadzeniu oraz przetwarzaniu pojawia się problem zagwarantowania bezpieczeństwa z punktu widzenia zachowań i postaw pracowniczych. Dzieje się tak dlatego, że postęp technologiczny wyprzedza w tym zakresie przygotowanie pracowników do użytkowania nowoczesnych instrumentów bezpieczeństwa. Celem artykułu jest przedstawienie podstawowych elementów społecznego wymiaru bezpieczeństwa informacyjnego organizacji. Punktem wyjścia w rozważaniach jest omówienie przykładowych zachowań pracowniczych sprzyjających – jak również zagrażających – zachowaniu poufności posiadanych zasobów informacyjnych. Zaprezentowane zostały przykładowe działania członków organizacji, którzy, kierując się indywidualnymi korzyściami, przy niskim poziomie świadomości skutków swoich czynów kreowali sytuacje zwiększające poziom zagrożenia utraty kluczowych zasobów informacyjnych. W dalszej części publikacji omówiono model kultury organizacyjnej Edgara H. Scheina, wzbogacony o pojęcie „bohaterów organizacyjnych" zaproponowanym przez Geerta Hofstedego. Przybliżone zostały wskazania o sposobie i sile wpływu kultury organizacyjnej na funkcjonowanie członków przedsiębiorstwa. W ostatniej części publikacji zaprezentowano koncepcję subkultury organizacyjnej, którą jest kultura bezpieczeństwa informacji wraz z omówieniem przykładowych działań służących jej kształtowaniu i rozwojowi.

Słowa kluczowe: bezpieczeństwo informacyjne organizacji, kultura organizacyjna, postawy i zachowania pracownicze, kultura bezpieczeństwa informacji

Forming the elements of organisational culture aimed at maintaining information security
Abstract

Nowadays, in management, emphasis is put on the assumption that the key factors for business success are well-used intangible assets, which include a type of knowledge based on information that plays an enormous role, which in turn is formed on the basis of data that take the form of giant collections (so-called 'big data'). Their acquisition, collection and processing poses the risk guaranteeing safety from the point of view of behaviours and attitudes. This is because technological progress stays ahead of the employees' preparation for the use of modern security instruments in this area. The goal of the paper is to provide the basic elements of the social dimension of information security for an organisation. The starting point for the considerations is the discussion of examples of employee behaviours that are conducive and also endangering the confidentiality of information resources. The paper provides examples of the activities of members of an organisation who, guided by individual benefits, with a low level of awareness of the effects of their actions, have created situations that have increased the risk of losing key information resources. Subsequently, the paper discusses the model of organisational culture as suggested by Edgar H. Schein with its enrichment of the concept "organizational heroes", proposed by Geert Hofstede. The indications of the method and the power of the impact of organisational culture on the functioning of the members of the company were approximate. The final part of the paper presents the concept of organisational subculture, which rests on information security culture, together with the analysis of examples of actions aimed at its shaping and development.
Key words: information security of the organization, organizational culture, employee attitudes and behaviours, information security culture

Формирование элементов организационной культуры, направленных на обеспечение информационной безопасности
Резюме

В настоящее время в исследованиях, касающихся вопросов управления, подчеркивается, что доминирующими, ключевыми факторами успеха предприятий являются эффективно используемые нематериальные ресурсы. Среди них огромную роль играют знания, основанные на информации, формирующейся на основе данных, взятых из гигантских собраний (так называемые big data). Во время поиска, накопления и обработки этих данных, возникает проблема обеспечения безопасности, связанная с поведением сотрудников. Эта проблема имеет место в связи с тем, что технологический прогресс опережает возможности подготовки персонала в сфере пользования современными инструментами безопасности. В статье представлены основные элементы социального измерения информационной безопасности организации. Отправной точкой исследования было рассмотрение примеров поведения сотрудников, способствующих или угрожающих конфиденциальности информационных ресурсов. Автор наводит примеры действий сотрудников организаций, которые, руководствуясь индивидуальными выгодой и низким уровнем информированности о последствиях своих действий, создали ситуации, повышающие

уровень угрозы утери ключевых информационных ресурсов. В статье рассмотрены модели организационной культуры Эдгара Шейна (введенное им понятие организационных героев). Эта модель является продолжение разработки Герта Хофстеде. В исследовании показано также возможности и силу влияния организационной культуры на функционирование сотрудников предприятия. В последней части публикации представлено концепцию субкультуры организации, которой является культура безопасности информации. Были также рассмотрены примеры действий направленных на формирование и развитие культуры безопасности информации.
Ключевые слова: безопасность, информационные организации, организационная культура, поведение сотрудников, культура безопасности информации