NASK
Cyber POLICY

Analiza

Psychologiczne aspekty cyberbepieczeństwa

Paweł Zegarow

Kwiecień 2019

www.cyberpolicy.nask.pl

Psychologiczne aspekty cyberbezpieczeństwa

Mimo dynamicznego rozwoju systemów zabezpieczeń informatycznych liczba przestępstw popełnianych w cyberprzestrzeni stale rośnie. Jak wynika z raportu przygotowanego przez ***Center for Strategic and International Studies i McAfee*** w 2018 roku, **straty spowodowane przez nielegalną działalność w cyberprzestrzeni osiągnęły rekordowy poziom 445-608 mld dolarów**, co stanowiło 0,59 - 0,8 % światowego produktu krajowego brutto. Według ekspertów to istotny wzrost w porównaniu z danymi z 2014 roku (345-445 mld dolarów).[1]

Do najszybciej rozwijających się zagrożeń w cyberprzestrzeni zalicza się obecnie ataki ransomware, wykorzystujące szkodliwe oprogramowanie szyfrujące dane i blokujące dostęp do systemu komputerowego. Cyberprzestępcy coraz częściej wykorzystują też pewne formy psychologicznej manipulacji i metody inżynierii społecznej, przed którymi nie chronią użytkowników zabezpieczenia informatyczne. Mimo że przestrzeganie stosunkowo prostych zasad pozwala uniknąć dużej części incydentów, wielu użytkowników wciąż nie dba w wystarczającym stopniu o swoje bezpieczeństwo w sieci. Tymczasem zrozumienie mechanizmów odpowiedzialnych m.i n. za ocenę bezpieczeństwa jest pierwszym krokiem do podejmowania racjonalnych decyzji w sieci.

Wzrost znaczenia nauk społecznych i czynnika ludzkiego w cyberbezpieczestwie

W obliczu rosnącego zagrożenia ze strony ataków, wyorzystujących niedoskonałości funkcjonowania l udzkiego umysłu, to właśnie czynnik ludzki odgrywa decydującą rolę w cyberbezpieceństwie. Frederick R.Chang, były dyrektor ds. badań w NSA, już w 2012 roku twierdził, że kwestie cyberbezpieczeństwa muszą być rozpatrywane zarówno na gruncie nauk ścisłych, jak i społecznych.[2]

Podobne podejście można zaobserwować w dzia- NATO, które w odpowiedzi na potrzeby zgłaszane przez **Supreme Allied Command Transformation (SACT) i Human Intelligence Center of Excellence (HUMINT COE) stworzyło NATO** Innovation Hub, będący przestrzenią wymiany doświadczeń i wyników badań z zakresu cyberpsychologii.

[1] Lewis, J. (2018). Economic Impact of Cybercrime - No Slowing Down Report. McAfee: Santa Clara, CA, USA.
[2] Chang, F. R. (2012). Guest Editor's Column. The Next Wave, 19(4): 1–2.

Czym zajmuje się cyberpsychologia?

Cyberpsychologia to owa subdyscyplina psychologii, która opisuje mechanizmy rządzące ludzkim umysłem i zachowaniem w kontekście nowych technologii. Mimo stosunkowo krótkiej, bo liczącej blisko 20 lat tradycji badawczej, cyberpsychologia dostarczyła już wielu praktycznych wskazówek prawiających bezpieczeństwo.

Obecne badania koncentrują się na psychologicznych konsekwencjach korzystania z cyberprzestrzeni, rzeczywistości wirtualnej i rozszerzonej, sztucznej inteligencji i innych innowacji cyfrowych, które stopniowo docierają do coraz większej grupy użytkowników. Nauka ta z jednej strony umożliwia zrozumienie postępowania człowieka w relacji z technologią, a z drugiej bada wpływ technologii na zachowania społeczne poszczególnych jednostek, grup i organizacji.

Cyberpsychologia bazująca na odkryciach tradycyjnej psychologii zyskuje coraz większe znaczenie w nowoczesnym społeczeństwie. Szczególnym obszarem zainteresowania jest czynnik ludzki w cyberbezpieczeństwie, a najciekawsze wydają się badania nad czynnikiem ludzkim w kontekście tzw. cyberhigieny.

Cyberhigiena – definicja i rola czynnika ludzkiego

W literaturze naukowej istnieją liczne definicj terminu „cyberhigiena", które podkreślają złożony i interdyscyplinarny charakter tego pojęcia. Można spośród nich wyodrębnić te, które akcentują behawioralny albo techniczny aspekt cyberbezpieczeństwa. Dodatkowo oba podejścia mogą być rozpatrywane na poziomie jednostkowym lub organizacyjnym. W zależności od zainteresowań badawczych autora, definicje cyberhigieny dotyczą zmiany zachowania (czynnik ludzki) lub wdrażania środków technicznych zwiększających cyberbezpieczeństwo (czynnik technologiczny).

Według Keith Kirkpatrick cyberhigienę należy rozumieć, jako „wdrażanie i egzekwowanie polityki ochrony prywatności i bezpieczeństwa danych, procedur i kontroli w celu zminimalizowania ryzyka potencjalnych szkód i naruszenia bezpieczeństwa danych".[3]

Inne rozumienie proponują Virgilio F. Almeida wraz z zespołem badawczym, którzy traktują cyberhigienę, jako zbiór najlepszych praktyk, dotyczących bezpiecznego korzystania z sieci i ochrony urządzeń podłączonych do Internetu.[4] Termin cyberhigiena często występuje również w publikacjach nieakademickich. W tekstach prawnych i rządowych autorzy często przedstawiają istotę cyberhigieny przez analogię do higieny osobistej.[5][6] Podobnie jak mycie rąk chroni przed chorobami układu pokarmowego, tak samo m.in. regularne zmiany unikalnych haseł chronią przed nieuprawnionym dostępem do kont poczty elektronicznej czy serwisów społecznościowych. Mimo braku jednolitej definicji, **cyberhigiena jest zwykle rozumiana, jako zbiór zasad, zachowań i zaleceń, których przestrzeganie zwiększa cyberbezpieczeństwo indywidualnych użytkowników i organizacji.**

Przestrzeganie zasad cyberhigieny pozwala uniknąć dużej części incydentów. Niestety wielu internautów na co dzień wciąż nie stosuje dobrych praktyk bezpiecznego korzystania z sieci. Mimo licznych ostrzeżeń, użytkownicy swobodnie dzielą się hasłami do różnych serwisów i usług za pomocą poczty elektronicznej, udostępniają prywatne informacje w serwisach społecznościowych czy realizują operacje bankowe poprzez nieznane otwarte sieci wi-fi. Może to wynikać z kilku powodów.

Autorzy raportu *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity* z ENISA podkreślają, że przez ostatnie 25 lat działania zwiększające bezpieczeństwo komputerowe koncentrowały się głównie na technicznym zabezpieczaniu systemów i urządzeń. Rola człowieka w systemie bezpieczeństwa była ograniczona przez procedury i sankcje.[7] Strategia ta mogła przyczynić się do niskiego poziomu świadomości społecznej na temat profilaktyki ataków w cyberprzestrzeni.

[3] Kirkpatrick, K. (2015). Cyber policies on the rise. Communications of the ACM, 58(10), 21-23Clara, CA, USA

[4] Almeida, V. A., Doneda, D., & de Souza Abreu, J. (2017). Cyberwarfare and digital governance. IEEE Internet Computing, 21(2), 68-71.

[5] Review of cyber hygiene practices. ENISA, Heraklion (2016). http://publications. europa. eu/ publication /manifestation_identifier /PUB_TP0217008ENN Maennel, K., Mäses, S., & Maennel, O. (2018).

[6] Cyber Hygiene: The Big Picture. In Nordic Conference on Secure IT Systems (pp. 291-305). Springer, Cham.

[7] Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, https:// www.enisa.europa.eu/publications/cybersecurity-culture

Kolejnym powodem jest brak właściwej edukacji w tym obszarze. Badacze sugerują, że użytkownicy często nie rozumieją istoty działań zwiększających cyberbezpieczeństwo, co może prowadzić do przyjmowania biernej postawy.[8][9] Żeby lepiej zrozumieć problem przestrzegania zasad bezpiecznego korzystania z sieci, należy zacząć od sposobu postrzegania bezpieczeństwa i psychologicznych konsekwencji tego procesu.

Postrzeganie bezpieczeństwa w cyberprzestrzeni, czyli dlaczego błędnie oceniamy potencjalne zagrożenia?

Pojęcie bezpieczeństwa w cyberprzestrzeni może być rozumiane w aspekcie obiektywnym (matematycznym) i subiektywnym (psychologicznym).

Bezpieczeństwo w rozumieniu **obiektywnym** opiera się na matematycznej interpretacji prawdopodobieństwa i umożliwia określenie, jak bardzo bezpieczny jest dany system lub użytkownik, biorąc pod uwagę działające na niego czynniki ryzyka.[10]

Bezpieczeństwo w aspekcie **subiektywnym** opiera się na psychologicznych r eakcjach, występujących w sytuacjach ryzyka i kontroli. Oba czynniki są równie ważne, przenikają się i wymagają interdyscyplinarnego podejścia.

W literaturze naukowej funkcjonuje pogląd, że każdy może zupełnie inaczej postrzegać ryzyko niezależnie od tego, jaki jest jego rzeczywisty poziom. Prawidłowość ta dotyczy również użytkowników sieci. Na proces postrzegania ryzyka wpływa szereg czynników osobowościowych, wcześniejsze doświadczenia, zniekształcenia poznawcze, priorytety i system wartości danej jednostki.[11] Przykładowo, jeśli bezpieczeństwo w sieci jest priorytetem lub ważną wartością, to istnieje duże prawdopodobieństwo, że dany użytkownik będzie zwracał większą uwagę na cyberbezpieczeństwo niż osoba, dla której kwestia bezpieczeństwa w sieci jest mało istotna.

Paradoksalnie, użytkownik może odczuwać wysoki poziom dyskomfortu z powodu s ubiektywnego poczucia zagrożenia, mimo niskiego prawdopodobieństwa ataku. Przykładem może być sytuacja, w której internauta z obawy przed wystąpieniem incydentu, całkowicie rezygnuje np. z korzystania z systemu bankowości elektronicznej lub inwestuje w bardzo kosztowne programy ochrony. Mówi się wtedy o przecenianiu zagrożenia, które jest subiektywne.

Z drugiej strony użytkownik może czuć się w pełni bezpiecznie, pobierając nielegalne oprogramowanie z sieci, mimo że nie tylko łamie prawo, a le obiektywnie zwiększa prawdopodobieństwo zainfekowania urządzenia złośliwym oprogramowaniem. W takim przypadku można mówić o bagatelizowaniu zagrożenia. Złudne poczucie bezpieczeństwa połączone z przekonaniem o anonimowości może prowadzić do nieprzestrzegania podstawowych zasad bezpiecznego korzystania z sieci. Tego rodzaju przekonania „wyłączają" świadomość cyberbezpieczeństwa.

Pięć tendencji oceny ryzyka

Bruce Schneier w książce „Beyond fear: thinking sensibly about security in an uncertain" wymienia pięć tendencji w ocenie ryzyka, którym ulegamy :[12]

1. Wyolbrzymiamy ryzyko wystąpienia zdarzeń spektakularnych, ale stosunkowo rzadkich i bagatelizujemy ryzyko wystąpienia zdarzeń powszechnych, ale mniej spektakularnych.

    a. Przykład: wyolbrzymianie prawdopodobieństwa kradzieży tożsamości i zaniżanie prawdopodobieństwa zaszyfrowania danych przez złośliwe oprogramowanie w celu wyłudzenia pieniędzy.

2. Mamy trudność z oszacowaniem ryzyka wystąpienia zdarzeń, które odbiegają od sytuacji, z którymi mamy do czynienia na co dzień.

[8] Dhillon, G., & Backhouse, J. (2001). Current directions in ISsecurity research: towards socio organizational perspectives. Information Systems Journal, 11(2), 127-153.

[9] Hu, Q., Hart, P., & Cooke, D. (2006, January). The role of external influences on organizational information security practices: An institutional perspective. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol.6,pp. 127a-127a). IEEE.

[10] Schneier, B. (2008). The psychology of security. In International Conference on Cryptology in Africa (pp. 50 - 79). Springer, Berlin, Heidelberg

[11] Y. Asnar and N. Zannone, "Perceived risk assessment," in 4th ACM workshop on Quality of protection, 2008, pp. 59–64.

[12] Schneier, B. (2006). Beyond fear: Thinking sensibly about security in an uncertain world. Springer Science & Business Media.

a. Przykład: trudność w oszacowaniu prawdopodobieństwa ataku ransomware po pobraniu plików z nieznanych źródeł, jeśli nigdy nie spotkaliśmy się z takim zagrożeniem i mamy bardzo niski poziom wiedzy o cyberbezpieczeństwie.

3. Zawyżamy ryzyko wiązane z działaniami konkretnej osoby, a zaniżamy ryzyko związane z działaniami osób nieznanych, anonimowych.

   a. Przykład: wyolbrzymianie prawdopodobieństwa wyrządzenia szkody przez znanych użytkowników forum dyskusyjnego, a zaniżanie prawdopodobieństwa wyrządzenia szkody przez osoby, z którymi dana osoba się nie zna.

4. Zawyżamy ryzyko związane z sytuacjami, których nie możemy kontrolować i zaniżamy ryzyko działań, które chętnie podejmujemy.

   a. Przykład: wyolbrzymianie prawdopodobieństwa kradzieży pieniędzy z konta po ustawieniu przelewów okresowych (opłata za telefon, Internet, tv), a zaniżanie prawdopodobieństwa kradzieży pieniędzy z konta podczas zakupu towarów w niezwykle atrakcyjnych cenach z nieznanego sklepu internetowego.

5. Przeceniamy ryzyko zdarzeń, które są przedmiotem publicznej dyskusji .

   a. Przykład: okresowe zwiększenie czujności i bezpiecznych zachowań w sieci w trakcie trwania kampanii społecznych, emitowania spotów czy wystąpień ekspertów.[13] Opisane tendencje wpływają na podjęcie decyzji o przestrzeganiu zasad cyberhigieny. Zrozumienie tych zjawisk może pomóc użytkownikom. podejmować bardziej świadome i racjonalne decyzje.

[13] Schneier, B. (2006). Beyond fear: Thinking sensibly about security in an uncertain world. Springer Science & Business Media.

Nadmierny optymizm

Kolejnym czynnikiem, który wpływa na niewłaściwą ocenę bezpieczeństwa w sieci, jest błąd poznawczy nazwany w literaturze naukowej „nadmiernym optymizmem"[14]. Liczne badania wykazały, że ludzie przejawiają nadmierny optymizm w stosunku do postrzeganego ryzyka. Jak wynika z pracy Neila D. Weinstin'a, jesteśmy silnie przekonani, że doświadczymy większej liczby zdarzeń pozytywnych i mniejszej liczby zdarzeń negatywnych niż inni ludzie[15]. Można założyć, że internauci także ulegają nadmiernemu optymizmowi – nie doceniają prawdopodobieństwa wystąpienia negatywnych zdarzeń. .

Takie przekonanie w wielu przypadkach może wpływać na ignorowanie zagrożeń i brak działań zwiększających bezpieczeństwo. Paradoksalnie użytkownicy mają świadomość, że mogą paść ofiarami cyberprzestępców, ale są silnie przekonani, że tak się nie stanie. Wielu z nich nie przestrzega zasad cyberbezpieczeczeństwa, lecz nie ponosi natychmiastowych konsekwencji swoich działań – a to jeszcze bardziej wzmacnia złudne poczucie bezpieczeństwa. Przykładem może być pochopne pobieranie i otwieranie nietypowych plików z poczty e-mail bez wcześniejszego przeskanowania programem antywirusowym.

Heurystyki

Kolejnym przykładem upraszczającym nasze postrzeganie świata są heurystyki, które w przeciwieństwie do algorytmów, są prostymi i oszczędzającymi czas regułami myślenia[16]. Termin „heurystyka" opisywany w pracach Daniela Kahneman'a i Amosa Tversky'ego definiuje się, jako uproszczony model wnioskowania probabilistycznego, który sprzyja szybkiemu formułowaniu sądów bez szczegółowej analizy wystarczającej ilości informacji. Rozumowanie to opiera się na subiektywnej ocenie prawdopodobieństwa zaistnienia realnej sytuacji[17]. Kahneman i Tversky po przeprowadzeniu serii badań eksperymentalnych, które dostarczyły wiedzy na temat niedoskonałości. .wnioskowania ludzkiego umysłu, wyodrębnili trzy następujące heurystyki: .

- **dostępności,**
- **zakotwiczenia,**
- **reprezentatywności.**

[14] Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016, April). College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. In 2016 Cybersecurity Symposium (CYBERSEC) (pp.68-73). IEEE.

[15] Weinstein, N. D. (1989). Optimistic biases about personal risks. Science, 246(4935), 1232-1234.

[16] Wojciszke, B. (2009). Człowiek wśród ludzi: zarys psychologii społecznej. Wydawnictwo Naukowe Scholar.

[17] Kahneman, D., Slovic, S. P., Slovic, P., & Tversky, A. (Eds.). (1982). Judgment under uncertainty: Heuristics and biases. Cambridge university press.

Opisane heurystyki mają charakter ogólny i mogą pomóc lepiej zrozumieć zachowania użytkowników w cyberprzestrzeni.[18]

a) heurystyka dostępności

Heurystyka dostępności polega na ocenie częstości lub prawdopodobieństwa wystąpienia zdarzeń w oparciu o łatwość, z jaką przychodzą nam na myśl przykłady tych zdarzeń i jak silnie są nacechowane emocjonalnie.[19] Jeśli w niedalekiej przeszłości osoba z naszego najbliższego otoczenia padła ofiarą cyberprzestępców, to może nam się wydawać, że zjawisko cyberprzestępczości zagraża nam znacznie bardziej niż kiedykolwiek. Analogicznie, jeśli nie słyszymy o takich przypadkach, to mamy tendencje do bagatelizowania zagrożeń związanych z cyberprzestępczością.

Heurystyka dostępności zwykle pozwala na wydawanie trafnych sądów, ponieważ z darzenia, które występują często, są łatwo dostępne ludzkiej świadomości (o takich zdarzeniach zwykle słyszymy w mediach, są to zdarzenia silnie nacechowane emocjonalnie). Zdarza się jednak, że heurystyka dostępności zawodzi, ponieważ nie wszystkie informacje dostępne świadomości odnoszą się do zdarzeń częstych.

Profesor Bogdan Wojciszke w książce „Człowiek wśród ludzi: zarys psychologii społecznej" podaje następujący przykład działania tej heurystyki: „co jest częstszą przyczyną śmierci w Polsce, zabójstwa czy samobójstwa?". Intuicyjnie większość ludzi odpowiada, że częstszą przyczyną śmierci w Polsce są zabójstwa.

Tymczasem w Polsce w wyniku zabójstw ginie blisko tysiąc osób rocznie, a życie odbiera sobie blisko 5 tys. osób.[20] Informacje o zabójstwach są znacznie częściej podawane do publicznej wiadomości (bardziej dostępne świadomości). Samobójstwa są zjawiskiem obiektywnie częstszym, ale mniej medialnym (mniej dostępne świadomości). Heurystyka dostępności opiera się więc na subiektywnym uczuciu łatwości uświadomienia sobie jakiejś informacji.

Stosowanie tej heurystyki może prowadzić do efektu konfirmacji, czyli błędu poznawczego polegającego na wybieraniu informacji, które potwierdzają wcześniej przyjęte oczekiwania. Przykładem jest osoba, która nie instaluje oprogramowania antywirusowego, ponieważ osoby z jej najbliższego otoczenia nie używają tego rodzaju programów i nie padły ofiarą cyberprzestępców. Strategia ta może prowadzić do nieracjonalnych zachowań, które zagrażają bezpieczeństwu.

b) heurystyka zakotwiczenia

Heurystyka zakotwiczenia polega na ocenie prawdopodobieństwa, częstości czy liczby przypadków danego zdarzenia, w oparciu o łatwo dostępną informację tzw. kotwicę (podaną przez media, rozmówcę lub niedawno zasłyszaną), którą następnie modyfikujemy w oparciu o własną wiedzę i kontekst sytuacyjny. Zmiana ta w wielu przypadkach jest pozorna, a sądy formułowane są w kierunku, który sugeruje łatwo dostępna informacja.

Wojciszke podaje następujący przykład działania tej heurystyki: „rozważmy sytuacje kupowania domu i oceny, jaka jest jego rzeczywista wartość".[21] Kupujący domyśla się (wiedza i kontekst), że pośrednik nieruchomości zawyża wartość domu, ale cena (kotwica) podana przez niego jest punktem wyjścia do formułowania sądu na temat rzeczywistej wartości domu. Biorąc pod uwagę własną wiedzę, kontekst i cenę podaną przez pośrednika, jesteśmy w stanie za pomocą heurystyki zakotwiczenia oszacować rzeczywistą wartość domu. Należy podkreślić, że wyższy poziom wiedzy na dany temat, osłabia efekt działania heurystyki zakotwiczenia, ponieważ daje większą liczbę przesłanek do myślenia racjonalnego. Zdaniem Wojciszke wyższy poziom wiedzy nie zapewnia jednak pełnej ochrony.

Stosowanie tej heurystyki może prowadzić do błędu poznawczego polegającego na ignorowaniu prawdopodobieństwa wystąpienia pewnych zdarzeń. Przykładem jest osoba, która wie, że wchodzenie na niektóre strony internetowe oferujące oglądanie np. seriali, wiąże się z prawdopodobieństwem zainfekowania komputera złośliwym oprogramowaniem, ale ignoruje ten fakt i wciąż korzysta z tego rodzaju stron.

[18] Nęcka, E., Orzechowski, J., & Szymura, B. (2008). Psychologia poznawcza. Wydawnictwo Szkoły Wyższej Psychologii Społecznej" Academica".

[19] Wojciszke, B. (2009). Człowiek wśród ludzi: zarys psychologii społecznej. Wydawnictwo Naukowe Scholar.

[20] Wojciszke, B. (2009). Człowiek wśród ludzi: zarys psychologii społecznej. Wydawnictwo Naukowe Scholar.

[21] Wojciszke, B. (2009). Człowiek wśród ludzi: zarys psychologii społecznej. Wydawnictwo Naukowe Scholar.

c) heurystyka reprezentatywności

Heurystyka reprezentatywności polega na ocenie przynależności danego obiektu do kategorii, opierając się na podobieństwie tego obiektu do typowych przedstawicieli kategorii[22]. Stosowanie tej heurystyki jest efektywną strategią odpowiadania na istotne pytania np. kto lub co należy do danego zbioru. Osoby stosujące heurystykę reprezentatywności ignorują prawidłowości statystyczne, sugerując się kryterium podobieństwa, a nie prawdopodobieństwem wystąpienia danego zdarzenia czy zjawiska.

Heurystyka reprezentatywności jest często błędnie stosowana w odniesieniu do teorii spiskowych, które przez pozorne podobieństwo pewnych elementów (np. powtarzające się katastrofy lotnicze nad danym terytorium) są uważane za ściśle ze sobą powiązane, celowe i wysoce prawdopodobne. Osoba stosujące tę heurystykę ignoruje np. takie czynniki jak pogoda, stan techniczny samolotów, dyspozycje pilotów i wiele innych mogących mieć wpływ na katastrofę lotniczą. Heurystyka ta opiera się na podobieństwie i prowadzi do poszukiwania przyczyn w zdarzeniach podobnych.

Heurystyka reprezentatywności pomaga zrozumieć proces wyłudzania danych przez cyberprzestępców, którzy wykorzystują metodę tzw. phishingu. Użytkownik banku otwiera e-mail, który ma wszelkie cechy wcześniejszej korespondencji (logo, czcionka, styl) i przekonany o prawdziwości tej wiadomości (otrzymana wiadomość jest typowa i podobna do poprzednich) wykonuje żądaną przez cyberprzestępców akcję. Stosowanie heurystyki reprezentatywności istotnie zmniejsza ilość czasu potrzebną do podjęcia decyzji, ale zwiększa też podatność na ataki phishingowe.

Podsumowanie

1. W ostatnich latach obserwuje się **wzrost zainteresowania „czynnikiem ludzkim" w cyberbezpieczeństwie** zarówno wśród przedstawicieli nauk społecznych, jak i międzynarodowych organizacji.

2. **Liczba przestępstw popełnianych w cyberprzestrzeni stale rośnie**, a cyberprzestępcy coraz częściej wykorzystują w atakach pewne formy psychologicznej manipulacji, przed którymi nie chronią użytkowników systemy zabezpieczeń informatycznych.

3. Jednym z największych wyzwań stojących obecnie przed cyberpsychologią jest **edukowanie i zwiększanie świadomości użytkowników** w zakresie psychologicznych aspektów cyberbezpieczeństwa.

4. **Zrozumienie procesów odpowiedzialnych za m.in. podejmowanie decyzji czy ocenę zagrożenia**, z których nie zawsze zdajemy sobie sprawę, jest pierwszym krokiem do wzięcia odpowiedzialności za własne bezpieczeństwo w sieci.

[22] Wojciszke, B. (2009). Człowiek wśród ludzi: zarys psychologii społecznej. Wydawnictwo Naukowe Scholar.