# Cyberpsychologia: klucz do lepszej obrony organizacji

**Liczba cyberprzestępstw stale rośnie, a ofiarami ataków padają organizacje posiadające pozornie doskonałą infrastrukturę bezpieczeństwa. Stosowane przez cyberprzestępców techniki manipulacyjne pomagają skutecznie realizować ataki, przed którymi nie chronią nawet najlepsze systemy. Psychologia cyberbezpieczeństwa pozwala zrozumieć motywy działania cyberprzestępców oraz przewidzieć ich kolejne kroki, dzięki czemu organizacje mogą lepiej przygotować się na ewentualne zagrożenie.**

## Profil cyberprzestępcy

Cyberpsychologia stanowi nową dziedzinę psychologii obejmującą zagadnienia psychologiczne związane z pojawiającą się technologią. Nauka ta bada ludzkie zachowania w kontekście interakcji z cyberprzestrzenią i pozwala prowadzić analizy dotyczące zachowań i motywów cyberprzestępców, dzięki którym możliwe będzie przewidzenie kolejnych zachowań osób stojących za cyberatakami.

Naukowcy badający motywy oraz sposoby postępowania cyberprzestępców ustalają sylwetkę przestępcy, podobnie jak odbywa się to w psychologii kryminalnej. Psychologiczna ocena określa zestaw cech prawdopodobnie wspólnych dla osób popełniających wybrany rodzaj przestępstw. Według powszechnie dostępnych informacji za najpowszechniejsze motywy cyberprzestępców uznaje się: chęć zdobycia pieniędzy, chęć zabawy, motywy emocjonalne i osobiste, a także motywy polityczne, ideologiczne oraz religijne.

W zależności od motywu, sylwetka przestępcy może się różnić, jednak będą oni mieli kilka cech wspólnych. Kim zatem jest statystyczny cyberprzestępca? Wbrew pozorom, wcale nie musi to być jednostka wybitnie inteligentna. Klasyczny cyberprzestępca charakteryzuje się przeciętną inteligencją, niespełnionymi ambicjami oraz trudnością w nawiązywaniu kontaktów międzyludzkich. Za cechy charakterystyczne dla większości cyberprzestępców uznaje się posiadanie wiedzy technicznej, nihilizm prawny, wysoką tolerancję na ryzyko, potrzebę manipulowania innymi oraz potrzebę potwierdzenia własnej wartości. W przypadku organizacji nierzadko sprawcą ataku okazuje się być obecny lub były pracownik. Taka osoba ma wiedzę dotyczącą struktury firmy oraz stosowanych w niej zabezpieczeń, co pozwala na podejmowanie bardziej skutecznych działań.

## Jakie taktyki manipulacji stosują cyberprzestępcy?

Jak pokazuje sylwetka statystycznego cyberprzestępcy, jest to przeważnie osoba o średnim poziomie inteligencji. Nie przeszkadza to jednak w skutecznym manipulowaniu otoczeniem, poprzez bazowanie na ludzkich instynktach.

– *Cyberprzestępcy doskonale zdają sobie sprawę z istnienia skutecznych systemów zabezpieczeń, dlatego oprócz umiejętności technicznych wykorzystują standardowe metody, przed którymi żaden system nie jest w stanie zabezpieczyć człowieka: manipulują, straszą i pospieszają. To właśnie dzięki strachowi i presji czasowej przestępcom udaje się skutecznie przeprowadzać ataki ransomware – grożenie utratą danych w przypadku niezapłacenia okupu w wyznaczonym czasie zmusza ofiary do podejmowania szybkich, niekoniecznie dobrych decyzji* – wyjaśnia Jakub Król, System Engineer w Simplicity Sp. z o.o.

Cyberprzestępcy nieustannie wykorzystują taktyki psychologiczne do osiągania własnych celów. Stosowanie socjotechnik pozwala im nakłonić ofiary do wyjawienia tajnych informacji lub podjęcia określonych działań, na przykład wejścia na podejrzaną stronę czy podania danych logowania na stronę banku. Nierzadko dzieje się to przy jednoczesnym wywieraniu presji czasowej i wywoływaniu strachu.

## Sposoby na wzmocnienie strategii obronnych w organizacji

Organizacje są w stanie skutecznie bronić się przed atakami cyberprzestępców, jednak wymaga to nieustannego prowadzenia szeregu działań. Kluczową rolę w ochronie danych mają zarówno rozwiązania techniczne (na przykład systemy bezpieczeństwa), jak i rozwiązania organizacyjne (na przykład regularne szkolenia oraz budowanie atmosfery zaufania).

– *Stosowanie odpowiednich zabezpieczeń pozwala organizacjom uniknąć chaosu związanego ze stosowaną przez cyberprzestępców presją czasu oraz manipulacją. Wzmocnieniem strategii obronnych będzie wykorzystanie systemów takich jak IPS, UBA, APT czy SIEM. Wykrywanie zagrożeń w czasie rzeczywistym oraz błyskawiczna reakcja systemów na zidentyfikowany atak daje organizacji czas na podjęcie rozsądnych działań obronnych* – wyjaśnia ekspert z Simplicity Sp. z o.o.

Cyberprzestępcy bazują na pierwotnych ludzkich instynktach, dlatego ważne jest również zadbanie o bezpieczeństwo w wewnętrznej społeczności tworzonej w organizacji. Przede wszystkim należy szkolić pracowników oraz podnosić ich świadomość na temat zagrożeń i działań, jakie powinni podejmować w przypadku nieoczekiwanej sytuacji. Warto też kształtować kulturę organizacji, w której – zgodnie z powiedzeniem, że lepiej kilka razy się pomylić, niż raz nie zareagować – zgłaszanie nieprawidłowości oraz zadawanie pytań nie będzie uznawane za niekompetencję i brak wiedzy, a proaktywną postawę godną pochwały.

Kontakt dla mediów:

Małgorzata Knapik-Klata

PR Manager

tel. 509 986 984

e-mail: m.knapik-klata@commplace.com.pl