Czynnik ludzki w cyberbezpieczeństwie firmowym

Kaspersky Security Awareness

kaspersky AKTYWUJ PRZYSZŁOŚĆ

Dowiedz się więcej na kaspersky.pl/awareness

Uwzględnianie czynnika ludzkiego ma kluczowe znaczenie dla cyberbezpieczeństwa korporacyjnego

Teraz, gdy organizacje instalują zaawansowane filtry phishingowe i zapory sieciowe oraz wdrażają specjalistyczne narzędzia w celu złagodzenia skutków cyberzagrożeń, cyberprzestępcy skupili się na pracownikach jako początkowym punkcie wejścia do systemów informatycznych. Wykorzystywanie typowych luk w wiedzy użytkowników to najłatwiejszy sposób na penetrację korporacyjnej infrastruktury IT.

Błąd ludzki - główne źródło cyberincydentów

Według Kaspersky i międzynarodowych badań B2B, **52% firm** przyznaje, że pracownicy są najsłabszym punktem bezpieczeństwa IT, z nieostrożnymi działaniami, brakiem wiedzy zaburzają korporacyjną strategię bezpieczeństwa IT.

Według raportu Wombat z 2018 r. dotyczącego ryzyka związanego z użytkownikiem, **55% pracujących dorosłych** umożliwia znajomym i członkom rodziny dostęp do urządzeń służbowych, które posiadają w domu, a **66% respondentów**, którzy nie używają narzędzia do zarządzania hasłami, przyznaje, że ponownie wykorzystuje 60% swoich haseł dla innych kont w internecie.

60% pracowników ma poufne dane na swoim urządzeniu firmowym (dane finansowe, bazy danych, pocztę e-mail itp.), a **30% pracowników** przyznaje, że udostępnia współpracownikom login i hasło do swojego komputera służbowego.[1]

Według raportu firmy Verizon o naruszeniach danych z 2018 r. **4% ludzi** nadal uważa, że kliknięcie podejrzanego załącznika to nic wielkiego.

Pracownicy stali się głównym celem cyberprzestępczości - wykorzystywanie ludzkich słabości takich jak nieuwaga, ignorancja czy zaniedbanie jest o wiele łatwiejsze i tańsze niż próba oszukania zaawansowanego oprogramowania zabezpieczającego.

W ubiegłym roku **67% kradzieży poświadczeń** powiodło się dzięki nieostrożności pracowników, którzy dali się nabrać na oszustwa phishingowe.[2]
Błędy lub przypadkowe zdarzenia są obecnie odpowiedzialne za **21% wszystkich naruszeń bezpieczeństwa**.[3]

Według badania Shred-it przeprowadzonego przez Ipsos, prawie połowa **kadry zarządzającej (47%)** i jeden na trzech **właścicieli małych firm (31%)** odnotował błąd ludzki lub przypadkowe ujawnienie danych przez pracownika / osobę posiadającą dostęp do informacji poufnych jako przyczynę naruszenia danych.

Brytyjskie Biuro Komisarza ds. Informacji (ICO) zgłasza, że **88% naruszeń danych** w Wielkiej Brytanii w ciągu ostatnich dwóch lat było spowodowanych błędem ludzkim, a nie atakami hakerów.

Biorąc pod uwagę wszystkie te statystyki, wiele organizacji pracujących nad budowaniem bezpiecznego środowiska korporacyjnego naturalnie stawia związane z nimi kwestie jako jeden z priorytetów do wzmocnienia i poprawy świadomości w zakresie cyberbezpieczeństwa.

„Zwiększyć szkolenie personelu, aby zapobiec nieostrożnym zachowaniom", jest **jednym z trzech najważniejszych priorytetów** zarządzania w 2019 r. dla **53% respondentów badania**, o którym mówi raport Instytutu Ponemon „Pomiar i zarządzanie cyberryzykiem dla działań biznesowych".

Żadna organizacja nie jest zbyt mała lub zbyt duża, aby nie stać się celem cyberprzestępców:

- w 2018 r. **43%** cyberataków było wymierzonych w małe firmy.[3]
- w 2017 r. naruszenie bezpieczeństwa Equifax, które ujawniło dane osobowe ponad **146 milionów** ludzi było wynikiem błędu ludzkiego, ponieważ pracownicy nie zastosowali się do ostrzeżeń i zasad bezpieczeństwa podczas wdrażania poprawek oprogramowania.

Średni wpływ finansowy niewłaściwych działań niedbałych / niedoinformowanych pracowników[4]

Dla małych i średnich firm

- średni roczny wpływ finansowy naruszeń danych spowodowanych niewłaściwym wykorzystaniem zasobów IT przez pracowników – **98 000 dolarów**
- fizyczna utrata urządzeń lub nośników należących do firmy - **105 000 dolarów**

Dla przedsiębiorstw

- średni roczny wpływ finansowy naruszeń danych spowodowanych niewłaściwym wykorzystaniem zasobów IT przez pracowników - **1 057 000 dolarów**
- fizyczna utrata urządzeń lub nośników należących do firmy - **1 416 000 dolarów**

Skuteczna świadomość bezpieczeństwa

Szkolenia są niezbędne do podnoszenia świadomości wśród pracowników - motywowania ich do zwracania uwagi na cyberzagrożenia i środki zaradcze, nawet jeśli początkowo nie jest to postrzegane przez nich jako część ich obowiązków zawodowych.

Niestety, wiele programów szkoleniowych w zakresie świadomości bezpieczeństwa jest bardzo mało skutecznych. Dlaczego tak się dzieje?

Szkolenie w zakresie świadomości bezpieczeństwa jest często postrzegane jako trudne, nudne i nieistotne. Pracownicy często:

- uważają takie szkolenie za zbyt skomplikowane i techniczne, aby warto było poświęcić na nie czas,
- nie dostrzegają związku pomiędzy swoimi działaniami a możliwymi konsekwencjami,
- uważają, że dbanie o cyberbezpieczeństwo nie jest ich zadaniem, a specjalistów IT.

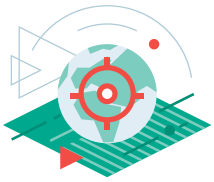
Bez względu na powód obojętności pracowników na oferowane szkolenia, efekt końcowy jest taki sam – ich zachowania nie zmieniają się.

Faktem jest również, że programy szkoleniowe są często zbyt krótkie, więc nie ma czasu na zgłębienie zdobytej wiedzy lub są zbyt czasochłonne i trudne do ukończenia oraz zawierają zbyt dużo dodatkowych lub nieistotnych informacji.

Szkolenie może również okazać się nieskuteczne, jeśli pracownicy czują się tak przytłoczeni instrukcjami dotyczącymi tego, co powinni, a czego nie powinni robić, że nie są w stanie tego wszystkiego przyswoić i nie wierzą w powodzenie - kwestie cyberbezpieczeństwa są postrzegane jako ograniczenia i przeszkody w radzeniu sobie z pracą.

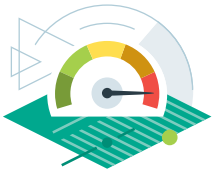
1 "Sorting out a Digital Clutter", Kaspersky, 2019.
2 "Measuring & Managing the Cyber Risks to Business Operations", Ponemon Institute LLC, Dec 2018
3 "2019 Data Breach Investigations Report" Verizon
4 "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives", Kaspersky, 2018

Skuteczny program szkoleniowy w zakresie świadomości bezpieczeństwa musi obejmować 4 kluczowe elementy:



Szkolenie ukierunkowane na role
- dowiedz się, co powinieneś wiedzieć, w oparciu o swoją rolę i profil ryzyka
- przykłady z życia wzięte i umiejętności, które można natychmiast wykorzystać
- nauka przez praktykę

Zorientowane na człowieka
- szkolenie zorganizowane zgodnie z naturalnym sposobem myślenia ludzi
- nadanie pozytywnego, proaktywnego spojrzenia na bezpieczne zachowanie
- informacje i umiejętności, które są łatwe do przyswojenia i zapamiętania dzięki metodologiom opartym na specyfice ludzkiej pamięci



Ciągłe przyrostowe uczenie się
- od łatwych do bardziej złożonych
- poszerzanie i stosowanie wcześniej zdobytej wiedzy w nowych kontekstach

Łatwość zarządzania i kontroli
- online
- zautomatyzowane zarządzanie nauką
- zaproszenia i wiadomości motywacyjne z indywidualnymi zaleceniami dla każdego ucznia wysyłane automatycznie

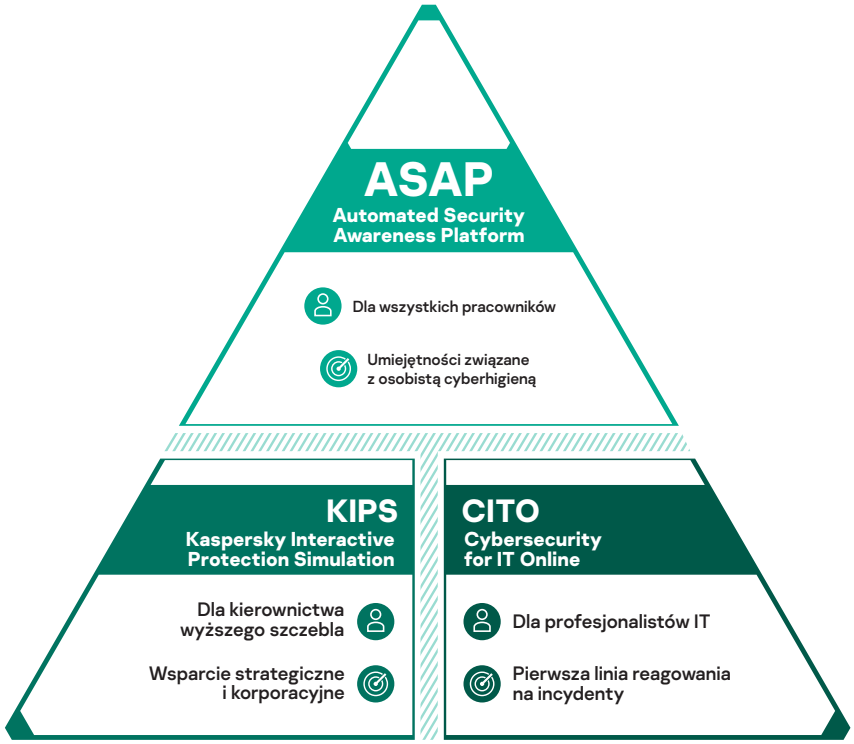
Zrozumienie, co kryje się za każdym procesem uczenia się i nauczania pomaga zbudować skuteczny program edukacyjny. Nasze programy nie tylko dostarczają wiedzy, ale - co ważniejsze - zmieniają nawyki i kształtują nowe wzorce zachowań, które są prawdziwym celem treningu świadomości.

Firma Kaspersky oferuje komputerowe produkty szkoleniowe, które łączą wiedzę z zakresu cyberbezpieczeństwa z najlepszymi praktykami w zakresie technik i technologii edukacyjnych. Takie podejście zmienia zachowanie użytkowników i pomaga stworzyć cyberbezpieczne środowisko w całej organizacji.

Kaspersky Security Awareness na świecie

- **75** krajów
- **580** organizacji
- **550 000** osób przeszkolonych do tej pory

Szkolenie Kaspersky Security Awareness



Ochrona dla korporacji: www.kaspersky.pl/korporacje
Kaspersky Security Awareness: www.kaspersky.pl/awareness
Darmowa wersja próbna oprogramowania ASAP: asap.kaspersky.pl

www.kaspersky.pl

kaspersky