Grant Thornton

Partner:

RESILIENTX

Cyberbezpieczeństwo uczelni wyższych

Jak dbamy o bezpieczeństwo studentów i ośrodków naukowych?

Analiza wycieków i podatności 50 najważniejszych uczelni w Polsce

Czerwiec 2026

Kluczowe wnioski

Uczelnie stają się celem cyberataków

W sieci dostępnych jest niemal 25 tys. wycieków danych powiązanych z 50 przebadanymi przez nas uczelniami wyższymi. W ich infrastrukturze wykryliśmy również ponad 59 tys. podatności, z czego zdecydowana większość miała status High lub Critical wg CVSS.

Skala zagrożeń rośnie szybciej niż poziom zabezpieczeń

Analiza wykazała, że głównym źródłem ryzyka są podatności infrastrukturalne obejmujące m.in. systemy sieciowe, serwery, usługi dostępne przez internet oraz środowiska wykorzystywane przez studentów i pracowników uczelni.

Szczególnie narażone są uczelnie przetwarzające dane wrażliwe

Wysoki poziom podatności odnotowano również na uczelniach medycznych, które poza standardowymi danymi studentów i pracowników przetwarzają także informacje związane z działalnością kliniczną, badaniami i ochroną zdrowia. Potencjalne skutki cyberataku mogą więc wykraczać daleko poza sam wyciek danych.

O badaniu

Badanie zostało przeprowadzone wśród 50 uczelni wyższych w Polsce. Analiza polegała na sprawdzeniu:

- ile dostępnych jest w sieci wycieków danych, tj. unikalnych haseł powiązanych z adresami e-mail w domenach badanych uczelni (jedno hasło traktowano jako jeden wyciek, nawet jeśli pojawiało się wielokrotnie lub było dostępne w wielu źródłach),
- ile widocznych podatności występuje w infrastrukturze każdej uczelni, z podziałem na podatności infrastrukturalne i webowe.

Jako podatności przyjęliśmy definicję zgodną z CVSS (Common Vulnerability Scoring System), opracowywaną przez organizację FIRST.org. Zebrane dane pochodzą z monitoringu pasywnego i zostały przygotowane dla Grant Thornton Technology przez firmę ResilientX.

W trosce o bezpieczeństwo badanych podmiotów celowo nie publikujemy szczegółowych informacji umożliwiających identyfikację konkretnych podatności ani potencjalnych wektorów ataku.

Dark web pełen danych uwierzytelniających

Polskie uczelnie nadal nie zapewniają odpowiedniej ochrony swoich systemów IT. Większość odnotowała znaczące wycieki danych logowania.

Według naszej analizy, w sieci dostępnych jest obecnie blisko 25 tys. wycieków danych uwierzytelniających użytkowników uczelni. Niechlubny rekordzista, jedna z dużych publicznych uczelni, posiada ponad 1400 zidentyfikowanych wycieków, co może świadczyć o wieloletnich zaniedbaniach w obszarze zarządzania dostępem i bezpieczeństwem kont. Mowa tu przede wszystkim o danych dostępowych wykorzystywanych w publicznych serwisach, do których rejestrowano się przy użyciu adresu mailowego uczelni.

Na szczęście, większość wykrytych wycieków ma stosunkowo niski poziom ryzyka. Oznacza to, że dane pojawiły się w sieci już jakiś czas temu albo są dostępne jedynie w pojedynczych źródłach. Nie oznacza to jednak, że problem można bagatelizować. W analizowanej grupie wykryliśmy również 71 wycieków o podwyższonym poziomie ryzyka. Są to przede wszystkim dane, które trafiły do sieci niedawno lub dostępne są wielu miejscach, przez co są znacznie łatwiej dostępne dla cyberprzestępców.

Przejęcie danych logowania nawet jednego pracownika lub studenta może stać się punktem wyjścia do dalszego ataku na infrastrukturę uczelni. Skala wykrytych wycieków pokazuje, że bezpieczeństwo kont i zarządzanie tożsamością cyfrową pozostają jednym z największych wyzwań dla polskiego szkolnictwa wyższego.

24996

wycieków łącznie

w tym o wadze:

niskiej	średniej	wysokiej
24925	48	23

Większa uczelnia = więcej danych

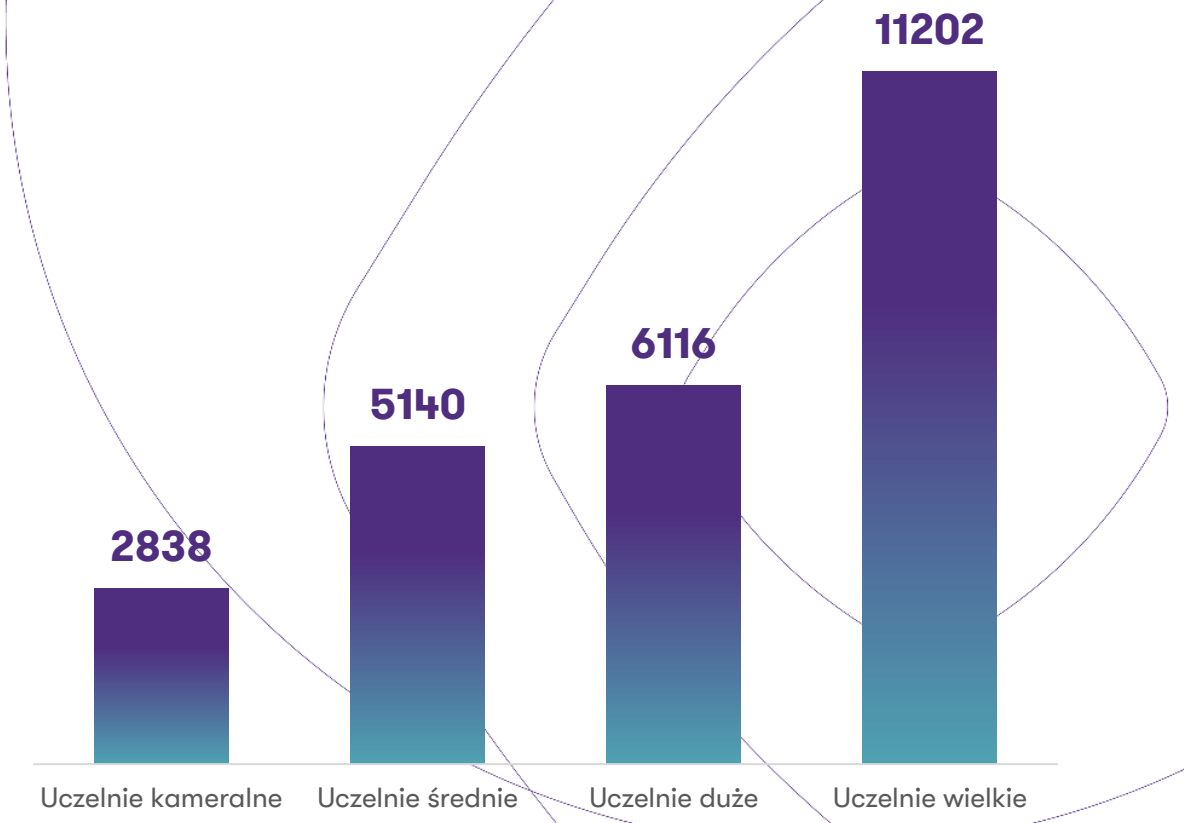
Zdecydowana większość wycieków danych logowania dotyczy największych polskich uczelni publicznych, posiadających rozbudowaną infrastrukturę IT oraz dziesiątki tysięcy aktywnych kont studentów, pracowników i współpracowników.

Ryzyko cyberataków rośnie wraz ze skalą organizacji. W przypadku największych uczelni liczba wykrytych wycieków przekraczała 1000 rekordów na pojedynczą instytucję. To właśnie w tej grupie odnotowaliśmy również największą liczbę incydentów o podwyższonym poziomie ryzyka.

Większa liczba wycieków w dużych uczelniach wynika przede wszystkim ze skali ich działalności: liczby użytkowników, systemów, usług cyfrowych oraz rozproszonej struktury organizacyjnej. Jednocześnie analiza pokazuje, że sama wielkość uczelni nie jest jedynym czynnikiem ryzyka. Wysoką liczbę podatności i wycieków odnotowaliśmy również w części mniejszych podmiotów, co może wskazywać na niedostateczny poziom zabezpieczeń lub mniejszą świadomość na temat zagrożeń.

Uczelnie wyższe, szczególnie największe i najbardziej zinformatyzowane, stają się coraz atrakcyjniejszym celem dla cyberprzestępców. Skala potencjalnych skutków ataku może obejmować nie tylko wyciek danych, lecz także zakłócenie działalności dydaktycznej, administracyjnej i badawczej.

Wykres 1. Liczba wycieków danych uwierzytelniających podzielona na kategorie uczelni: wielkie (od 25 tys. studentów), duże (od 13 tys. studentów), średnie (od 7 tys. studentów) i kameralne (poniżej 7 tys. studentów).



32

Liczba wycieków danych powiązanych z rektorami polskich uczelni

Nawet najważniejsze osoby na uczelniach są podatne na kradzież danych lub łamią zasady cyberhigieny

Podatności w uczelnianych systemach

Wycieki danych logowania to jednak tylko część problemu. Poważnym zagrożeniem są też podatności, czyli luki bezpieczeństwa w systemach wykorzystywanych przez uczelnie. Mogą prowadzić do cyberataków lub kolejnych wycieków.

Znacznie poważniejszym zagrożeniem są podatności, czyli luki bezpieczeństwa w systemach i usługach wykorzystywanych przez uczelnie, które mogą prowadzić do cyberataków lub kolejnych wycieków danych.

Według analizy przeprowadzonej dla Grant Thornton przez firmę ResilientX (w formie pasywnego skanu infrastruktury, a więc bez podejmowania prób przełamania zabezpieczeń) w 50 badanych uczelniach zidentyfikowano niemal 60 tys. podatności. Obejmują one zarówno infrastrukturę IT, jak i systemy oraz usługi dostępne z internetu. W praktyce mogą umożliwiać m.in. wykonanie złośliwego kodu, przejęcie kontroli nad systemem, dostęp do danych uwierzytelniających czy wykorzystanie błędów konfiguracyjnych. Szczególnie niepokojący jest poziom krytyczności wykrytych luk. Ponad 37 tys. podatności zostało sklasyfikowanych jako wysokie lub krytyczne zgodnie z metodologią CVSS (Common Vulnerability Scoring System). Oznacza to, że potencjalny atak może być stosunkowo łatwy do przeprowadzenia, a jego skutki bardzo poważne.

59499

podatności łącznie

w tym o wadze:

730	21686	22116	14967
niskiej	średniej	wysokiej	krytycznej

Podatności w infrastrukturze

W przeciwieństwie do wielu innych sektorów, największym problemem badanych uczelni nie okazały się podatności webowe, lecz luki występujące w infrastrukturze IT.

Podatności można traktować jako potencjalne punkty wejścia do systemów uczelni. Dzielą się one na dwie główne kategorie - podatności **webowe**, związane z aplikacjami i usługami dostępnymi z internetu, oraz podatności **infrastrukturalne**, dotyczące m.in. serwerów, urządzeń sieciowych, usług zdalnego dostępu czy systemów operacyjnych.

Nasza analiza wykazała, że zdecydowaną większość wykrytych luk stanowiły właśnie podatności infrastrukturalne. Oznacza to, że źródłem ryzyka są przede wszystkim rozbudowane i często trudne do zarządzania środowiska IT wykorzystywane przez studentów, pracowników i administrację.

Szczególnie niepokojący pozostaje jednak ogólny poziom krytyczności wykrytych luk. Znaczna część podatności została sklasyfikowana jako wysokie (22 tys. podatności) lub krytyczne (14 tys.), co oznacza, że potencjalne wykorzystanie ich przez cyberprzestępców może być stosunkowo proste i katastrofalne w skutkach.

Podatności **infrastrukturalne**:

58 650

w tym o wadze:

niskiej	średniej	wysokiej	krytycznej
730	**21686**	**22116**	**14118**

Podatności webowe

Podatności webowe stanowiły stosunkowo niewielką część wszystkich wykrytych luk bezpieczeństwa w badanych uczelniach, ale wszystkie miały wagę krytyczną.

Spośród niemal 60 tys. zidentyfikowanych podatności jedynie 849 dotyczyło systemów i aplikacji dostępnych bezpośrednio z Internetu, co stanowi około 1,4% wszystkich wykrytych problemów.

Zdecydowana większość podatności miała charakter infrastrukturalny – wykryliśmy ich ponad 58,6 tys. Oznacza to, że główne ryzyko dla uczelni nie wynika z samych stron internetowych czy aplikacji webowych, aczkolwiek wszystkie zbadane przez nas ryzyka miały najwyższą wagę. Choć ich liczba była relatywnie niewielka, część z nich mogła umożliwiać przejęcie dostępu do systemów, ujawnienie danych lub dalszą eskalację ataku.

Wykryte podatności webowe dotyczyły przede wszystkim błędów konfiguracyjnych, nieaktualnych komponentów oraz powszechnie wykorzystywanych technologii internetowych.

Źródłami wycieków są popularne adresy

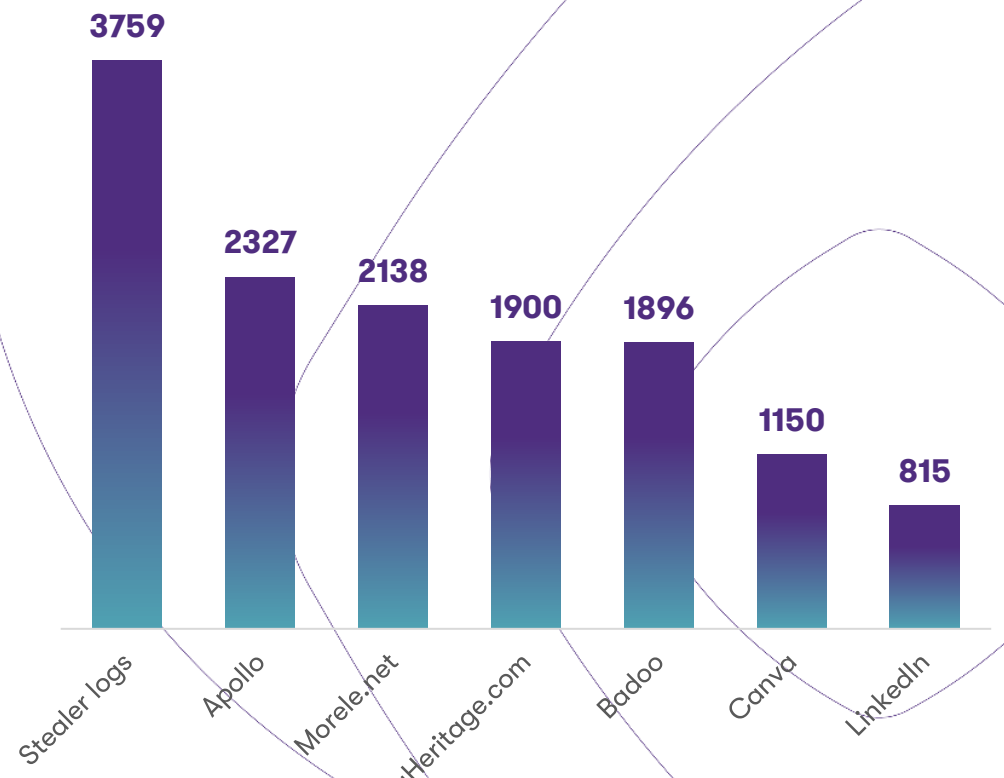
Analiza źródeł wycieków pokazuje, że znaczna część danych logowania trafia do sieci w wyniku naruszeń bezpieczeństwa w zewnętrznych serwisach internetowych, z których korzystają studenci i pracownicy.

Największym pojedynczym źródłem wycieków okazały się tzw. stealer logs – zbiory danych przechwyconych przez złośliwe oprogramowanie wykradające zapisane hasła, pliki cookie i dane przeglądarek. W badanej grupie odpowiadały one za blisko 3,8 tys. ujawnionych rekordów. Tego typu wycieki są szczególnie niebezpieczne, ponieważ często zawierają aktualne dane logowania do wielu różnych usług jednocześnie.

Drugim najczęściej występującym źródłem był wyciek związany z platformą Apollo (startup sprzedażowy), obejmujący ponad 2,3 tys. rekordów. Na trzecim miejscu znalazł się polski sklep internetowy Morele.net, którego historyczny incydent bezpieczeństwa odpowiadał za ponad 2,1 tys. ujawnionych danych powiązanych z użytkownikami uczelni.

Wśród najczęściej występujących źródeł znalazły się również wycieki pochodzące z serwisów MyHeritage, Badoo, Canva oraz LinkedIn. Pokazuje to, że bezpieczeństwo uczelni jest dziś w dużej mierze uzależnione od cyberhigieny samych użytkowników, którzy często używają tych samych haseł w różnych serwisach.

Wykres 2. Liczba wycieków danych wrażliwych powiązana z konkretnym źródłem.



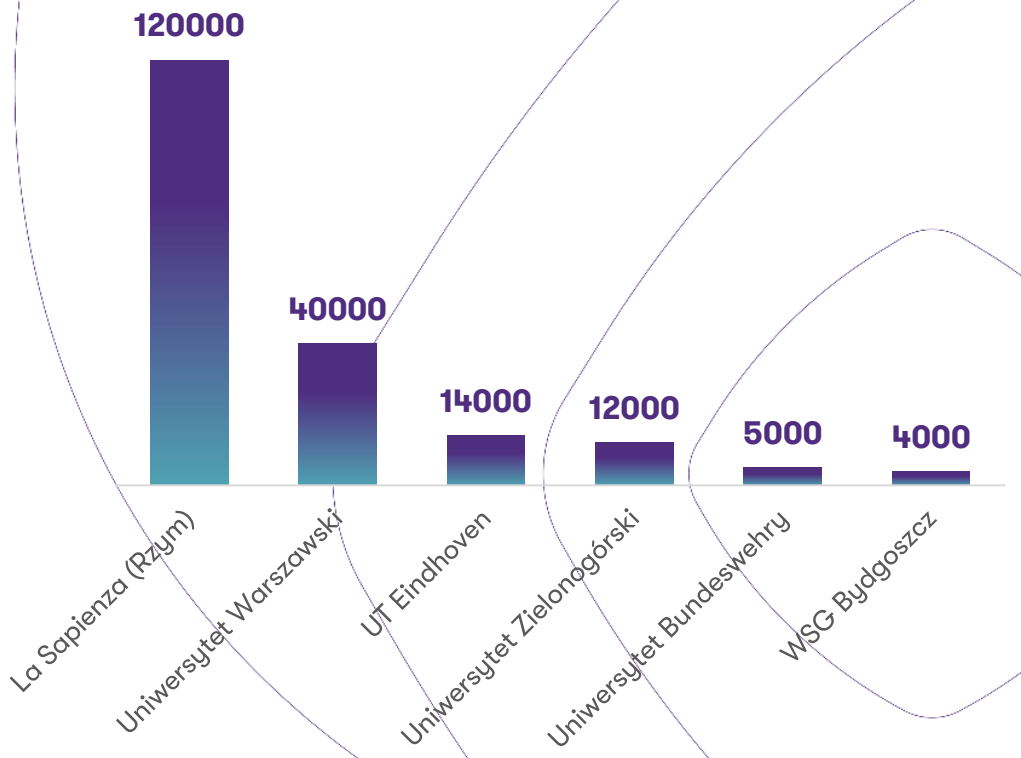
Ataki paraliżują uczelnie w całej Europie

Cyberataki na uczelnie wyższe przestały być incydentami o charakterze lokalnym i coraz częściej prowadzą do poważnych zakłóceń w ich działalności. W ostatnich latach głośne incydenty odnotowano zarówno w Europie, jak i w Polsce.

W 2026 r. ransomware sparaliżował Uniwersytet La Sapienza w Rzymie, największą uczelnię w Europie, powodując czasowe wyłączenie kluczowych systemów i zakłócenia w obsłudze studentów. Wcześniej podobne problemy dotknęły m.in. Uniwersytet Techniczny w Eindhoven oraz Uniwersytet Bundeswehry w Monachium, gdzie skutkiem ataków były wycieki danych i długotrwała odbudowa infrastruktury IT.

Polskie uczelnie również stają się celem coraz bardziej zaawansowanych działań cyberprzestępczych. Najpoważniejszym przypadkiem był incydent na Uniwersytecie Warszawskim, w wyniku którego cyberprzestępcy uzyskali dostęp do około 850 GB danych obejmujących dokumenty studentów, pracowników i kandydatów. Charakterystyczne dla tego ataku było wykorzystanie przejętych danych logowania oraz brak żądania okupu – celem było samo pozyskanie i upublicznienie danych. W ostatnich latach odnotowano również ataki ransomware na Uniwersytet Zielonogórski oraz Wyższą Szkołę Gospodarki w Bydgoszczy, które doprowadziły do czasowego ograniczenia dostępności usług i uruchomienia procedur kryzysowych.

Wykres 3. Liczba studentów uczelni dotkniętych najpoważniejszymi wyciekami danych w latach 2024-2026 (malejąco).



Źródło: Szacunek Grant Thornton na podstawie danych z publicznych źródeł

Okiem eksperta

Wyniki badania odnoszą się do zróżnicowanej grupy polskich uczelni, jednak ze względu na strukturę sektora szkolnictwa wyższego w dużej mierze odzwierciedlają sytuację uczelni publicznych. Analiza wskazuje również na wyraźną zależność między skalą działalności a poziomem narażenia na zagrożenia cybernetyczne – większe uczelnie częściej stają się celem ataków i odnotowują więcej incydentów.

Cyberbezpieczeństwo powinno być postrzegane nie tylko jako obszar regulowany przepisami, lecz także jako integralny element kontroli zarządczej. Tym bardziej niepokojące są utrzymujące się luki w zabezpieczeniach, mimo wieloletniego obowiązywania wymogów dotyczących bezpieczeństwa informacji i ciągłości działania.

Skala wykrytych wycieków danych oraz podatności pokazuje, że cyberbezpieczeństwo nie jest wyłącznie zagadnieniem technicznym, lecz jednym z kluczowych czynników wpływających na realizację podstawowych zadań uczelni. Szczególnie istotne jest to, że większość zidentyfikowanych podatności dotyczy infrastruktury informatycznej, co wskazuje na systemowy charakter ryzyka.

Wyniki badania podkreślają również znaczenie czynnika ludzkiego. Duża liczba wycieków danych uwierzytelniających wskazuje, że użytkownicy pozostają jednym z najważniejszych źródeł ryzyka, dlatego działania edukacyjne i budowanie kultury bezpieczeństwa powinny być traktowane na równi z zabezpieczeniami technicznymi.

W świetle standardów kontroli zarządczej cyberbezpieczeństwo powinno stanowić stały element zarządzania uczelnią, obejmujący identyfikację i ocenę ryzyka, raportowanie zagrożeń, monitorowanie skuteczności zabezpieczeń oraz wdrażanie działań korygujących. Wyniki badania należy zatem traktować nie tylko jako diagnozę stanu bezpieczeństwa technologicznego polskich uczelni, lecz także jako sygnał potrzeby dalszego rozwoju systemów zarządzania ryzykiem. W warunkach postępującej cyfryzacji odporność cybernetyczna staje się jednym z kluczowych mierników zdolności uczelni do realizacji swoich celów i zapewnienia ciągłości działania.

Dr Joanna Przybylska
Prof. UEP
Pełnomocnik Rektora ds. Koordynacji Kontroli Zarządczej

Naszym zdaniem

W dobie masowo ujawnianych podatności, wyciekających haseł i rosnącej liczby ataków na uczelnie wyższe na całym świecie, cyberbezpieczeństwo sektora akademickiego przestaje być wyłącznie kwestią techniczną – staje się warunkiem ciągłości działania, ochrony reputacji oraz bezpieczeństwa danych studentów, pracowników i partnerów badawczych.

Uczelnie są szczególnie atrakcyjnym celem dla cyberprzestępców, ponieważ łączą kilka wrażliwych obszarów: duże zbiory danych osobowych, systemy finansowe i kadrowe, własność intelektualną, wyniki badań, infrastrukturę laboratoryjną, a często także dostęp do międzynarodowych konsorcjów naukowych.

Obecne trendy pokazują, że atakujący coraz częściej wykorzystują nie tylko klasyczny phishing, ale także przejęte hasła, credential stuffing, podatności w systemach VPN, poczcie, platformach e-learningowych, systemach zarządzania tożsamością czy aplikacjach webowych. Coraz większym problemem są również ataki ransomware połączone z wyciekiem danych, czyli tzw. double extortion. Dla uczelni taki incydent może oznaczać nie tylko paraliż zajęć i administracji, ale też utratę wyników badań, naruszenie danych osobowych, konsekwencje prawne oraz spadek zaufania grantodawców, partnerów i studentów.

W tym kontekście istotne znaczenie ma dyrektywa NIS-2, która podnosi wymagania dotyczące zarządzania ryzykiem cyberbezpieczeństwa, raportowania incydentów, odpowiedzialności kierownictwa oraz bezpieczeństwa łańcucha dostaw. Nawet jeśli konkretna uczelnia nie zawsze będzie bezpośrednio objęta wszystkimi obowiązkami, NIS-2 wyznacza praktyczny standard należytej staranności.

Cyberbezpieczeństwo uczelni powinno być traktowane tak samo strategicznie jak bezpieczeństwo finansowe czy prawne – bo od niego zależy ciągłość nauczania, wiarygodność badań i zaufanie całego środowiska akademickiego. Zmiana modelu z reaktywnego na proaktywny jest dziś ogromnym wyzwaniem dla uczelni wyższych, zarówno pod kątem organizacyjnym, kulturowym jak i finansowym.

Adam Woźniak
Partner
Cybersecurity
Grant Thornton

Partner:

Szukasz nowych rozwiązań biznesowych?

Skontaktuj się z nami!

Adam Woźniak
Partner
Cybersecurity
Grant Thornton
T +48 600 805 785
E Adam.Wozniak@pl.gt.com

Kontakt dla mediów:

Jacek Kowalczyk
Dyrektor Marketingu i PR
Grant Thornton
T +48 505 024 168
E Jacek.Kowalczyk@pl.gt.com

Autor: Adam Woźniak, Jan Kietliński

O nas

Grant Thornton to jedna z wiodących organizacji audytorsko-doradczych na świecie, obecna w 157 krajach i zatrudniająca ponad 76 tys. pracowników.

W Polsce działamy od 1993 roku. Zespół 1200 pracowników wspiera naszych klientów w obszarach takich jak doradztwo podatkowe, finansowe, prawne i transakcyjne, audyt, czy outsourcing kadr i płac oraz outsourcing księgowości.

W skład grupy wchodzi m.in. **Grant Thornton Technology**, spółka specjalizująca się w doradztwie dla firm w zakresie outsourcingu IT i cyberbezpieczeństwa, obsługująca kilkaset przedsiębiorstw rocznie w całej Polsce.