PARTNER GENERALNY

BNP PARIBAS

FUNDATORZY NAGRODY

KOZMINSKI UNIVERSITY

Ministerstwo Cyfryzacji

W obliczu narastających wyzwań w cyfrowym świecie, gdzie Polska znajduje się w stanie „cyfrowej wojny", a liczba incydentów bezpieczeństwa bije kolejne rekordy, kluczowe staje się budowanie krajowego potencjału w dziedzinie cyberbezpieczeństwa. Największą luką nie jest brak funduszy czy sprzętu, lecz luka kompetencyjna, a jej wypełnienie wymaga zaangażowania wszystkich dostępnych talentów. W tym kontekście szczególną rolę odgrywa zwiększenie udziału kobiet w branży IT i security, która historycznie postrzegana była jako domena męska.

Mimo że statystyki pokazują postęp – udział kobiet w cyberbezpieczeństwie wzrósł w ciągu dekady z 10 do około 25 proc. – wciąż jesteśmy daleko od równowagi. W Polsce odsetek ten szacuje się na poniżej 20 proc. Inicjatywy takie jak konkurs Rising Star in Cybersecurity, organizowany od 2022 roku przez społeczność Cyber Women Community, stają się kluczowym narzędziem zmiany tego obrazu.

Konkurs ma na celu nie tylko uhonorowanie i wsparcie polskich specjalistek, ale przede wszystkim promowanie stworzonych przez nie innowacyjnych projektów i dobrych praktyk. To platforma, która przełamuje stereotypy, pokazuje różnorodność ścieżek kariery w cyberbezpieczeństwie i tworzy wzorce do naśladowania dla przyszłych pokoleń.

Niniejszy raport prezentuje sylwetki finalistek tegorocznej, czwartej edycji konkursu Rising Star in Cybersecurity oraz ich niezwykłe projekty. To historie kobiet, które swoją pracą, pasją i zaangażowaniem nie tylko realnie wzmacniają cyfrową odporność Polski, ale także udowadniają, że różnorodność perspektyw i kompetencji jest fundamentem skutecznej obrony w cyberprzestrzeni. Ich sukcesy są dowodem na to, że kobiety wnoszą do branży unikalne umiejętności, często kładąc większy nacisk na czynnik ludzki, komunikację i empatię, co uzupełnia tradycyjne, techniczne podejście do bezpieczeństwa.

Mamy nadzieję, że ich dokonania staną się inspiracją dla całej branży oraz dla kobiet, które dopiero rozważają karierę w tym fascynującym i kluczowym dla przyszłości sektorze.

Mariola Rauzer
Wiceprezes Zarządu Evention,
organizatora Cyber Women Community

SPIS TREŚCI

RISING STAR IN CYBERSECURITY

O KONKURSIE

Rising Star in Cybersecurity to konkurs, który ma uhonorować a jednocześnie zaoferować dodatkowe wsparcie dla kobiet w cyberbezpieczeństwie w Polsce. Ma również promować stworzone przez panie dobre praktyki i innowacyjne projekty cybersecurity.

Konkurs skierowany jest do specjalistek, asystentek i menedżerek, ale nie na stanowiskach dyrektorskich, które w ciągu ostatnich 18 miesięcy przeprowadziły skuteczną transformację lub szkolenie, zrealizowały zakończoną sukcesem ciekawą inicjatywę albo projekt mający realny wpływ na rozwój świadomości i wiedzy o cyberbezpieczeństwie.

Do udziału w konkursie zapraszamy Panie, które:

- **stworzyły ciekawy projekt** związany z szeroko pojętym cyberbezpieczeństwem **lub mają ciekawą inicjatywę**, którą chcą zrealizować **w obszarze cybersecurity**
- **zajmują stanowiska specjalistek, asystentek lub managerek** z wyłączeniem stanowisk dyrektorskich

CO OCENIAMY?

Projekt lub działania, które miały istotny wpływ na rozwój wiedzy o cyberbezpieczeństwie, wykrytych podatnościach lub zabezpieczeniach.

Szukamy projektów, które w **innowacyjny sposób** zmieniły podejście do ochrony przed cyberzagrożeniami.

Zgłoszenia mogą dotyczyć różnych dziedzin: ochrony danych poufnych, zachowania ciągłości działania, a także działań edukacyjnych związanych z cyberbezpieczeństwem

DLACZEGO WARTO WZIĄĆ UDZIAŁ W KONKURSIE?

Oferujemy wsparcie mentorskie:
Każda z uczestniczek, które zakwalifikują się do rundy finałowej otrzyma wsparcie Magdaleny Petryniak - międzynarodowej konsultantki ds. komunikacji, sprzedaży doradczej i wywierania wpływu, założycielki Story Seekers Polska. Ekspertka pomaga finalistkom w przygotowaniu angażującego przemówienia, dobraniu najlepszych środków wyrazu i budowaniu pewności siebie na scenie.

KOZMINSKI UNIVERSITY

Stawiamy na nagrody, które mają wspierać rozwój i inspirować do dalszego działania.

Nagrodą główną w konkursie jest miejsce na rocznych studiach podyplomowych zarządzanie cyberbezpieczeństwem na **Akademii Leona Koźmińskiego**.

PARTNER GENERALNY KONKURSU

BNP PARIBAS

FUNDATORZY NAGRODY

KOZMINSKI UNIVERSITY

Ministerstwo Cyfryzacji

PATRONI KONKURSU

WOMEN IN TECHNOLOGY · fi it · Canada · ISACA Warsaw Chapter · (ISC)² Official Chapter · ISSA Polska · kobietynauka.org · RISK & COMPLIANCE Platform Europe · security magazine · SEKURAK.PL

GALA RISING STAR IN CYBERSECURITY 2025 – TAK BYŁO

Już po raz czwarty kapituła konkursu Rising Star in Cybersecurity nagrodziła polskie specjalistki z branży ICT, wybierając najbardziej kreatywne projekty w obszarze cyberbezpieczeństwa. Wydarzenie organizowane od 2022 r. przez społeczność Cyber Women Community jest nie tylko formą eskpozycji wartościowych rozwiązań technologicznych, ale także – a może przede wszystkim – platformą promowania mocniejszej obecności kobiet w sektorze stereotypowo postrzeganym jako „męski".

Gala Rising Star in Cybersecurity 2025 odbyła się 29 maja w przestrzeniach konferencyjnych BNP Paribas Polska, partnera konkursu. Oficjalna część wydarzenia rozpoczęła się od prezentacji kluczowych wniosków płynących z „Badania płac w obszarze information security 2025". Projekt jest wspólną inicjatywą ISSA Polska oraz Evention, realizowaną w ramach społeczności dyrektorów bezpieczeństwa CSO Council, rozwijanej od ponad ośmiu lat. Karol Lewandowski, Executive Director w Standard Chartered Bank, członek Rady Programowej CSO Council, przedstawił dane o tym, jakie specjalizacje i kompetencje są dzisiaj cenione w procesach rekrutacyjnych, kogo dzisiaj szukają firmy w obszarze cyberbezpieczeństwa i jak zmienia się sam rynek.

Wnioski z raportu były przyczynkiem do debaty o dzisiejszym rynku pracy w cybersecurity w Polsce i jego perspektywach na najbliższe lata. W dyskusji, moderowanej przez Aleksandrę Karasińską, dyrektorkę Fundacji RASP, wzięli udział: Lech Lachowicz, Global Threat Defense Engineering Director w PepsiCo; Alicja Malok, Senior Director, Technology Perm w Hays; Maciej Orliński, dyrektor Biura CERT w BNP Paribas Bank Polska; Monika Pieniek, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji; Anita Wiesiołek-Németh, dyrektor departamentu cyberbezpieczeństwa w Aplikacje Krytyczne i Alina Zając, IT Security Manager/ Head of CERT PL w E.ON.

W gali wzięli udział goście specjalni – **Krzysztof Gawkowski**, wiceprezes rady ministrów i minister cyfryzacji; **Catherine Godin**, ambasador Kanady w Polsce; prof. dr hab. **Grzegorz Mazurek**, rektor

Akademii Leona Koźmińskiego i **Krzysztof Słotwiński**, dyrektor Pionu Bezpieczeństwa i Zarządzania Ciągłością Działania w BNP Paribas Bank Polska – którzy wygłosili inspirujące przemówienia.

Po krótkiej przerwie scena należała już do głównych bohaterek wieczoru: każda z pięciu finalistek konkursu Rising Star in Cybersecurity 2025 krótko zaprezentowała swój projekt.

Magdalena Gołębiowska, doktorantka w Katedrze Sztucznej Inteligencji Politechniki Wrocławskiej, omówiła założenia i działanie opracowywanego przez siebie systemu głosowej autoryzacji użytkownika, EmoSpeechAuth.

Renata Kania, główny specjalista ds. budowania świadomości i kultury bezpieczeństwa w T-Mobile, opowiedziała o platformie edukacyjnej dla pracowników, Cyber Know.

Anna Kroker, analityczka cyberbezpieczeństwa w EY, przedstawiła projekt transformacji procedur zarządzania ryzykiem stron trzecich (TPRM).

Wystąpienie Moniki Lewandowskiej, analityczki bezpieczeństwa IT w Banku Polskiej Spółdzielczości, poświęcone było wdrożeniu centralnego systemu reagowania i odpowiedzi na incydenty bezpieczeństwa w podmiotach zrzeszonych w BPS.

Julia Lisowska-Wenta, Senior Security Analyst w BNP Paribas przybliżyła genezę i założenia prowadzonego przez nią projektu edukacyjnego dla seniorów, w ramach którego wzmacnia odporność cyfrową osób starszych.

„W BNP różnorodność i równość szans jest dla nas ogromną wartością i w banku dbamy o to, żeby rozwijać kobiety. Jeżeli 20 proc. udziału kobiet to średnia dla branży cybersecurity, to my w BNP mamy to szczęście, że u nas ta średnia jest wyższa. Dziewczyny, trzymam za was kciuki. Wszystkie jesteście wygrane.

KRZYSZTOF SŁOTWIŃSKI,
CISO, BNP Paribas Bank Polska

WERDYKT JURORÓW

W trakcie kilkudziesięciominutowej przerwy na dyskusję i naradę jury zdecydowało o przyznaniu nagród i wyróżnień.

Zwyciężczynią czwartej edycji Rising Star in Cybersecurity została Magdalena Gołębiowska. Laureatka została uhonorowana pamiątkową statuetką oraz nagrodami ufundowanymi przez partnerów konkursu – miejscem na rocznych studiach podyplomowych na kierunku „Zarządzanie cyberbezpieczeństwem" na Akademii Leona Koźmińskiego, a także voucherem od Ministra Cyfryzacji na dowolne szkolenia podnoszące kwalifikacje z cyberbezpieczeństwa. Nagrody wręczyli Monika Pienik, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, prof. dr hab. Grzegorz Mazurek, Krzysztof Słotwiński oraz Monika Gliwka, laureatka ubiegłorocznej edycji konkursu.

Drugie miejsce zajęła Renata Kania. Nagroda, jaka przypadła jej w udziale, to dwudniowe szkolenie OSINT – rozszerzony kurs z zaawansowanego pozyskiwania szczegółowych informacji na temat ludzi i firm, realizowany przez ekspertów z serwisu Niebezpiecznik.pl. Nagrodę i statuetkę wręczyli Aneta Legenza, przedstawicielka jury konkursu oraz Wojciech Głażewski, Country Manager polskiego oddziału firmy Checkpoint.

Na trzecim stopniu podium znalazła się Monika Lewandowska, która odebrała zasłużone gratulacje i nagrodę od reprezentującej jury Moniki Tośty oraz Anny Paszkowskiej, dyrektor sprzedaży i marketingu w firmie Softinet. Monika Lewandowska zdobyła także nagrodę publiczności w prowadzonym równolegle do obrad jury głosowaniu online. Michał Hryciuk, wiceprezes zarządu ISACA Warszawa, wręczył laureatce ufundowaną przez to stowarzyszenie nagrodę – voucher na egzamin do wybranej przez nią certyfikacji ISACA z zakresu cyberbezpieczeństwa.

„Akademia Leona Koźmińskiego stara się być zupełnie inną szkołą wyższą, niż pozostałe. Naszą misję i nasz cel oddaje hasło „A new school for a new world". Jesteśmy bardzo zaangażowani, aby dostarczać najwyższej jakości edukację, która odpowiada na bieżące potrzeby – menedżerskie i specjalistyczne. Dlatego oferta studiów zarządzania cyberbezpieczeństwem dla laureatki Rising Star in Cybersecurity to coś więcej niż tylko edukacja, to misyjność. Reprezentując Akademię jestem zaszczycony i dumny, że możemy być z wami być po raz kolejny. Obiecuję, że w kolejnych edycjach konkursu też będziemy obecni.

PROF. DR HAB. GRZEGORZ MAZUREK, Akademia Leona Koźmińskiego

Dwie ostatnie finalistki, Julia Lisowska-Wenta i Anna Kroker, zostały uhonorowane wyróżnieniami, które odebrały z rąk przedstawicielek jury, Alicji Skraburskiej i Małgorzaty Bjørum.

Oficjalną część gali zwieńczyło wspólne pamiątkowe zdjęcie finalistek, jury i organizatorów konkursu. Kolejna edycja Rising Star in Cybersecurity już na wiosnę 2026 r.!

„Obrady jury były niezwykle inspirujące, ale zarazem bardzo wymagające. Miałyśmy wspaniałe dziewczyny – kandydatki, które swoją pasją, zaangażowaniem i kreatywnością zdobyły nasze serca. Wybór był bardzo trudny. Oceniałyśmy nie tylko aspekty techniczne, ale także kreatywność oraz potencjał realnego wpływu na obszar cyberbezpieczeństwa, czyli to, jak ich projekty mogą kształtować przyszłości. Cyberbezpieczeństwo to nie tylko wyzwanie, ale i wspólny cel, który powinien przyświecać wszystkim zaangażowanym w budowanie bezpieczniejszego świata

EWA PIŁAT, Chief Information Security Officer, IATA


IN CYBERSECURITY


.eu


ECURITY


DYPLOM
Magdaleny Gałęziowskiej


MedEstelle

RISING STAR IN CYBERSECURITY

1 MIEJSCE

MAGDALENA GOŁĘBIOWSKA

POLITECHNIKA WROCŁAWSKA

// Kiedy dojrzała pani do pomysłu związania swojej kariery ze światem IT?

Informatyką interesowałam się od ukończenia szkoły podstawowej, widząc jak mój tata zajmuje się tym. Związanie przyszłości z IT było naturalnym następstwem moich zainteresowań i ścieżki edukacyjnej jaką wybrałam z tego powodu. To był prosta decyzja.

// Jak narodził się pomysł na system EmoSpeechAuth?

Obszar, którym się zajmuję jest połączeniem moich głównych zainteresowań naukowych – automatycznego rozpoznawania emocji przez maszyny – oraz zainteresowań mojego promotora – szeroko pojętego cyberbezpieczeństwa. W ramach mojej rozprawy doktorskiej chcieliśmy połączyć te dwa obszary, ponieważ podczas studiów zainteresowałam się również cyberbezpieczeństwem. Okazało się, że w weryfikacji mówcy emocje stanowią słabość dla obecnie wykorzystywanych systemów.

// Co jest potrzebne do praktycznego użycia systemu? Jak przebiegają prace nad rozwojem projektu?

System nie jest samodzielnym produktem. Ma on regulować dostęp do innych platform, tak jak na przykład logujemy się do elektronicznej skrzynki pocztowej. Kod systemu oraz wytrenowany model jest udostępniony jako repozytorium na platformie GitHub, by każdy deweloper bądź naukowiec, który jest zainteresowany wykorzystaniem rozwiązania, mógł go użyć.

Nie jest to jednak gotowy system – to, co tworzymy w ramach badań, to fundamenty. Pokazujemy, że technologia działa i może być użyta w praktyce, ale nie jest to jeszcze gotowy produkt. Jeśli ktoś chce, może na tym zbudować własny system, dopracowany pod kątem jakości, bezpieczeństwa i zgodności z przepisami. Naszym celem jest przyspieszenie innowacji, a nie dostarczanie gotowych komercyjnych rozwiązań. Rozwój systemu w naukowym sensie oznacza dalsze badania nad ulepszonymi rozwiązaniami.

// Jak przyjęła pani zwycięstwo w konkursie Rising Star in Cybersecurity i co znaczy dla pani ta nagroda?

Wygrana była niespodziewana ze względu na charakter zgłoszonego projektu – nie jest to projekt komercyjny, a badania wykonane w kierunku rozwoju technologii, a w poprzednich edycjach zgłaszane były głównie projekty o charakterze biznesowym. Odebrałam to jako dowód, że także badania akademickie mogą

Magdalena Gołębiowska

Badaczka w obszarze sztucznej inteligencji i cyberbezpieczeństwa przy Katedrze Sztucznej Inteligencji Politechniki Wrocławskiej. Specjalizuje się w automatycznym rozpoznawaniu emocji, biometrycznej weryfikacji mówcy oraz detekcji deepfake'ów. Jej celem jest tworzenie rozwiązań, które zwiększają zaufanie społeczne do nowych technologii, przeciwdziałają cyfrowemu wykluczeniu oraz poprawiają jakość interakcji człowiek-komputer. Poza działalnością naukową angażuje się w inicjatywy promujące różnorodność w świecie technologii.

być dostrzegane i doceniane w szerszym kontekście cyberbezpieczeństwa.

Ta nagroda jest dla mnie ogromnym wyróżnieniem i motywacją, żeby dalej rozwijać swoje pomysły i pokazywać, że prace naukowe mogą realnie wpływać na przyszłość technologii.

// Czy ma pani wrażenie, że kobiety w informatyce muszą starać się bardziej? Co by pani radziła młodym adeptkom technologii i IT, jak zwiększyć szanse w tej branży?

W moim odczuciu narracja, jeśli chodzi o kobiety w informatyce zaczyna się zmieniać pozytywnie. Oczywiście to mocno zależy od środowiska, o którym mówimy i jest to czynnik bardzo subiektywny. Na kobiety w IT bardziej zwraca się uwagę, bo jest ich mniej. Z jednej strony wpływa to korzystnie, jeśli chodzi o tworzenie sieci kontaktów, bo łatwiej jest być zapamiętanym jako kobieta i wyróżnić się z tłumu, ale to wyróżnienie często pokrywa się z tym, że znajdzie się ktoś, kto będzie chciał zweryfikować twoją wiedzę i osiągnięcia.

Trzeba też zrozumieć, że będąc kobietą w IT, nie jest niczym złym być przeciętną – tak jak mamy mnóstwo męskich przeciętnych pracowników IT. Porzućmy tę presję, zmieńmy nasta-

MAGDALENA GOŁĘBIOWSKA

POLITECHNIKA WROCŁAWSKA

wienie. Młodym adeptkom radziłabym przede wszystkim wiarę w siebie i konsekwencję – nie bać się zadawać pytań, szukać wsparcia w mentorach i aktywnie budować swoją sieć kontaktów.

// Dlaczego w pani ocenie wciąż należy „ewangelizować" społeczeństwo, że kobiety mogą odnosić sukcesy jako naukowczynie i praktyczki w takich dziedzinach jak informatyka i cyberbezpieczeństwo?

Wydaje mi się, że ta „ewangelizacja" jest potrzebna przede wszystkim po to, by znormalizować obecność kobiet w branży. Wciąż funkcjonuje obraz informatyka jako mężczyzny, więc warto pokazywać różnorodne przykłady – żeby młode dziewczyny mogły się w kimś przejrzeć i uwierzyć, że to także dla nich jest naturalna ścieżka. Myślę, że im więcej kobiet w IT będzie widocznych, tym szybciej to przestanie być tematem samym w sobie i po prostu będziemy postrzegani przez pryzmat naszych kompetencji, a nie płci.

// Mówi pani, że jej naukowym marzeniem jest tworzenie rozwiązań, które podnoszą zaufanie społeczeństwa do technologii, szczególnie u osób dotkniętych cyfrowym wykluczeniem. Gdzie dostrzega pani największe potrzeby w tym zakresie?

Największą barierą, którą widzę, jest brak zaufania do systemów opartych na sztucznej inteligencji oraz brak umiejętności cyfrowych wśród osób starszych i wykluczonych technologicznie. Technologie są często postrzegane jako skomplikowane i „obce", a to rodzi nieufność. Dlatego widzę ogromną potrzebę tworzenia narzędzi prostych w obsłudze, intuicyjnych, które nie wymagają od użytkownika specjalistycznej wiedzy.

Drugą ważną kwestią jest przejrzystość – ludzie muszą wiedzieć, jak działa system i na jakich zasadach podejmuje decyzje. Uważam, że transparentność i edukacja to klucz do budowania zaufania. Moim marzeniem jest, aby nowe rozwiązania cyfrowe nie tylko były innowacyjne, ale też dostępne i zrozumiałe dla każdego – tak, aby technologia nie pogłębiała wykluczenia, lecz je zmniejszała.

Projekt zgłoszony do Rising Star in Cybersecurity

EmoSpeechAuth

Badania pokazują, że emocje mogą znacząco obniżać skuteczność systemów autoryzacji opartej na głosie. W momentach silnego wzburzenia zmienia się bowiem tempo mowy, barwa głosu, ton i intonacja, co utrudnia poprawną identyfikację użytkownika. Celem systemu EmoSpeechAuth (od emotion, speech i authentication) jest zwiększenie niezawodności autoryzacji głosowej w warunkach emocjonalnych. Architektura rozwiązania opiera się na dwóch głębokich sieciach neuronowych: jedna odpowiada za ekstrakcję cech związanych z tożsamością mówcy, druga analizuje stan emocjonalny użytkownika.

Obie reprezentacje są następnie łączone za pomocą modułu atencji, znanego z dużych modeli językowych. Pozwala to uzyskać ostateczną, wzbogaconą reprezentację głosu, wykorzystywaną w procesie autoryzacji. Dzięki takiemu podejściu skuteczność systemu znacząco wzrosła – w porównaniu z modelem bazowym, nieuwzględniającym informacji o emocjach, odnotowano poprawę o 36,98 proc.

Rozwiązanie jest dostępne publicznie na platformie GitHub, co umożliwia jego dalsze rozwijanie i praktyczne wykorzystanie. Zastosowanie systemu EmoSpeechAuth w obszarach wymagających najwyższego poziomu bezpieczeństwa – takich jak systemy alarmowe, policyjne, bankowe czy inne usługi krytyczne – mogłoby nie tylko zwiększyć poziom ochrony, lecz także poprawić komfort i intuicyjność korzystania z technologii biometrycznych.

KOMENTARZ

KRZYSZTOF GAWKOWSKI

WICEPREZES RADY MINISTRÓW, MINISTER CYFRYZACJI

Wszystkim organizatorkom i organizatorom społeczności Cyber Woman Community chciałem złożyć serdeczne gratulacje, bo to już czwarta edycja konkursu Rising Star in Cybersecurity i pracy, którą trzeba wykonać jest masa. A Wy ją wykonujecie. Bardzo się cieszę, że pomysły, które kiełkują w ramach Rising Star in Cybersecurity, ale też w ramach tej społeczności, mogą odgrywać ważną rolę na mapie działalności biznesowej. To dzięki takim inicjatywom można wyobrazić sobie swoją przyszłość w branży – budując startupy czy angażując się w rozwój sektora ICT.

Z dumą obserwuję rozwój marki Cyber Woman Community i konkursu Rising Star in Cybersecurity, które stają się częścią szerokiego krajobrazu inicjatyw w obszarze cyber. Mam głębokie przekonanie, że zmierzamy ku większemu udziałowi kobiet w branży ICT, a przede wszystkim ku partnerstwu – im więcej osób będzie zaangażowanych w cyberbezpieczeństwo, tym lepiej dla państwa.

Naszym wspólnym celem powinna być konsekwentna realizacja zobowiązań. Jednym z nich jest strategia cyfryzacji Polski do 2035 roku, zakładająca, że kobiety będą stanowiły ponad 35 proc. pracujących w branży ICT i cyberbezpieczeństwie.

Nie zapewnimy bezpiecznej Polski wyłącznie dzięki miliardowym inwestycjom czy wymianie przestarzałego sprzętu. Największą luką jest luka kompetencyjna. To brak specjalistów – także na poziomie lokalnym – stanowi dziś największe zagrożenie. Potrzebujemy pasji, determinacji i rosnącej obecności kobiet w branży, ponieważ tylko rozwój kompetencji ludzkich zapewni nam realne bezpieczeństwo.

Cieszę się, że wiele osób angażuje się w tę dziedzinę nie tylko zawodowo, ale też emocjonalnie, wspierając swoje środowisko. Mówię przede wszystkim o kobietach, które swoją siłą, charyzmą i oddaniem wnoszą ogromną wartość do branży.

Drogie Panie, dziękuję Wam za wszystko, co robicie – dla siebie, dla innych i dla państwa. W imieniu państwa proszę o jeszcze więcej. Trzymam kciuki, aby polskie cyberbezpieczeństwo było budowane przez kobiety i z kobietami.

Jak trafiła pani do cyberbezpieczeństwa i czy od początku była to świadomie obrana przez panią ścieżka zawodowa?

Moja droga w cyberbezpieczeństwie zaczęła się od… ludzi. Pewnego dnia znalazłam się na „zawodowym skrzyżowaniu" i musiałam zdecydować co dalej. Kieruje mną zawsze przekonanie, że najważniejszym ogniwem każdej organizacji nie jest system, procedura ani nawet technologia. Najważniejszy jest człowiek. To właśnie obszar cyberbezpieczeństwa zapalił dla mnie „zielone światło", by to podejście i swoje przekonanie tam zawodowo realizować.

Czy przypomina pani sobie jakieś szczególnie trudne wyzwania w trakcie prac nad Cyber Know, które trzeba było pokonać opracowując platformę? Czy długo musiała pani przekonywać zespół do tej idei?

Proces stworzenia Cyber Know wymagał zarówno ogromnej determinacji, jak i cierpliwości. To ogrom intensywnej współpracy ze wspaniałymi ludźmi, którzy wzięli udział w realizacji mojego pomysłu. Kluczowym wyzwaniem było nie tylko stworzenie kompleksowego narzędzia edukacyjnego, ale również zbudowanie przekonania wśród decydentów do inwestycji w rozwój kultury bezpieczeństwa opartej na świadomości pracowników. Moim głównym sukcesem i efektem pracy jest to, że ludzie, dla których stworzyłam ten produkt, zrozumieli swoje znaczenie w łańcuchu bezpieczeństwa, zrozumieli jak duży mają wpływ na nie i to, że każdy z nich jest swoim indywidualnym centrum ochrony.

Narzędzie początkowo funkcjonowało jako wewnętrzna platforma, a następnie przeszło w formę usługi, świadczonej klientom T-Mobile. To chyba najlepsze potwierdzenie potrzeby istnienia takiego narzędzia?

Dokładnie tak. Platforma miała na celu badać poziom świadomości bezpieczeństwa wśród pracowników T-Mobile i wpływać na jego podniesienie. Transformacja platformy z narzędzia dedykowanego pracownikom na usługę dla klientów zewnętrznych potwierdza, że rosnąca świadomość cyberzagrożeń wymaga innowacyjnych i skutecznych rozwiązań edukacyjnych. To pokazuje realną potrzebę rynku na narzędzia, które nie tylko edukują, ale także wzmacniają postawy i praktyki bezpieczeństwa na skalę całej organizacji i jej ekosystemu.

Renata Kania

Autorka Programu Security Awareness w T-Mobile Polska, którego celem jest budowanie świadomości i kultury bezpieczeństwa. Twórczyni edukacyjnych kampanii phishingowych i szkoleń. Pełni rolę liderki Zespołu Produktów Security oraz głównej specjalistki ds. Security Awareness w T-Mobile Polska. Odpowiada za rozwój i wdrażanie innowacyjnych rozwiązań z zakresu cyberbezpieczeństwa. Jej misją jest podnoszenie świadomości w zakresie bezpieczeństwa cyfrowego oraz dostarczanie produktów skutecznie chroniących klientów i organizacje przed cyberzagrożeniami.

// Jak postrzega pani wyróżnienie w konkursie Rising Star in Cybersecurity w kontekście prowadzonych przez siebie inicjatyw?

Wyróżnienie to jest dla mnie największym potwierdzeniem tego, że jestem we właściwym miejscu, tego, że moje przekonania znalazły miejsce w sferze zawodowej. Jest to dla mnie potwierdzenie efektywności podejmowanych przeze mnie działań oraz motywacja do dalszego rozwoju, by działać z satysfakcją dla siebie ale i dla bezpieczeństwa ludzi. Wyróżnienie to traktuję jako kolejny krok w budowaniu zaangażowanej społeczności ekspertów, którzy wspólnie przesuwają granice innowacji w cyberbezpieczeństwie, zwłaszcza w obszarze zwiększania świadomości i edukacji.

// Dlaczego tak istotne jest stawianie człowieka w centrum inicjatyw związanych z bezpieczeństwem?

Musimy pamiętać, że iluzją bezpieczeństwa jest pozostawianie go wyłącznie w rękach technologii. Bezpieczeństwo zawsze zaczyna się od świadomości, zaś cyberbezpieczeństwo zaczyna się od człowieka. Technologia nigdy nie zastąpi odpowiedzialnego i świadomego użytkownika. Stawianie człowieka

w centrum oznacza zrozumienie, że to ludzie podejmują decyzje i to właśnie ich wiedza, nawyki i postawy są pierwszą linią obrony przed naruszeniami bezpieczeństwa. Skuteczne inicjatywy muszą więc łączyć nowoczesne narzędzia z edukacją, wsparciem i zrozumieniem, które zmieniają kulturę organizacji od podstaw.

// Jakie działania radzi pani innym kobietom, które chciałyby spróbować swoich sił w tym obszarze, tradycyjnie postrzeganym jako „męski”?

Dla mnie praca w obszarze Security to codzienne budowanie mostów – między IT a pracownikami, między technologią a ludzkimi odruchami, między lękiem a zrozumieniem. Przede wszystkich podpowiedziałabym moim koleżankom, aby nie wątpiły w siebie, aby zawsze kierowały się tym co czują, aby kierowały się tym co według nich ma sens, aby się nie bały. Zachęcam do budowania wiedzy technicznej popartej praktycznymi doświadczeniami, ale także do rozwoju umiejętności miękkich, komunikacyjnych. Ważne jest, by aktywnie korzystać z programów mentoringowych i nie bać się podejmować wyzwań. Różnorodność perspektyw, którą wnoszą kobiety, jest nieoceniona i powinna być świadomie promowana.

// Jakie główne czynniki pani zdaniem stoją na przeszkodzie temu, by kobiet w cyberbezpieczeństwie – i szerzej w IT – było więcej? Jak sobie z nimi poradzić?

Największą barierą często jest stereotypowe postrzeganie IT jako „męskiej” branży oraz niedostateczna promocja kobiecych sukcesów. Ważne jest tworzenie środowisk wspierających, promocja programów dla kobiet i edukacja już na poziomie szkół, aby budować odwagę i motywację do wejścia do branży. Jestem przekonana, że praca i obszar, który się czuje i uwielbia może stać się pasją a nie tylko nazywanym powszechnie etatem.

Projekt zgłoszony do Rising Star in Cybersecurity
Cyber Know

Cyber Know to edukacyjna platforma wspierająca rozwój cyfrowej odporności użytkowników. Jej celem było „odczarowanie” wizerunku cyberbezpieczeństwa poprzez praktyczne ćwiczenia, dialog i partnerskie podejście, które pokazuje, że bezpieczeństwo jest wspólną odpowiedzialnością, a nie tylko zbiorem procedur.

CyberKnow oferuje aktywną formę edukacji, w której kluczową rolę odgrywa trening i praktyka. Platforma umożliwia m.in. automatyczne wysyłanie symulowanych wiadomości phishing i smishing, monitorowanie i analizę reakcji pracowników na te ataki oraz personalizowane przekierowanie do szkoleń z zakresu świadomości cyfrowej.

Model edukacyjny opiera się na trzech krokach: test – analiza – edukacja. Dzięki temu użytkownicy uczą się rozpoznawać zagrożenia w bezpiecznym, kontrolowanym środowisku, gdzie mogą popełniać błędy i wyciągać z nich wnioski bez ryzyka dla organizacji.

Efekty działania platformy są mierzalne. Dzięki regularnym kampaniom symulacyjnym pracownicy coraz skuteczniej weryfikują podejrzane wiadomości, przestają „klikać w ciemno”, unikając zachowań ryzykownych, a także uczą się prawidłowych procedur zgłaszania incydentów.

Dla Security Operation Center oznacza to nie tylko wzrost liczby zgłoszeń w trakcie kampanii edukacyjnych, lecz przede wszystkim rosnącą świadomość i aktywność pracowników. Zamiast być biernymi odbiorcami zasad, stają się aktywnymi uczestnikami budowania bezpieczeństwa organizacji.

KOMENTARZ

CATHERINE GODIN

AMBASADOR KANADY W POLSCE

Gratuluję społeczności Cyber Women Community stworzenia tak nowoczesnej i przyszłościowej platformy, która nie tylko promuje profesjonalną doskonałość, ale także przełamuje stereotypy płci, pokazując istotny wkład kobiet w tak wysoce wyspecjalizowaną dziedzinę, jaką jest cyberbezpieczeństwo.

Tego typu inicjatywy odgrywają kluczową rolę w kształtowaniu bardziej inkluzywnej i innowacyjnej przyszłości cyfrowej. Jest to dziś potrzebne bardziej niż kiedykolwiek wcześniej. Od momentu rosyjskiej inwazji na Ukrainę cyberbezpieczeństwo przestało być wyłącznie kwestią techniczną – stało się sprawą odporności narodowej i suwerenności.

Jako państwo graniczne Polska zmierzyła się z ogromnym wzrostem liczby incydentów cybernetycznych i odpowiedziała na nie z determinacją, wzmacniając krajową strategię cyberbezpieczeństwa, inwestując w infrastrukturę i budując wykwalifikowaną kadrę. Rozwój Polski w obszarze IT i cyberbezpieczeństwa jest niezwykły i naprawdę robi na mnie ogromne wrażenie. Z 295 tysiącami aktywnych programistów i 44 tysiącami studentów informatyki rocznie, Polska stała się jednym z największych dostawców talentów technologicznych w UE oraz znaczącym europejskim eksporterem usług IT do Ameryki Północnej, w tym do Kanady.

Kanada i Polska już dziś ściśle współpracują na arenie międzynarodowej w ramach wielu inicjatyw dotyczących cyberbezpieczeństwa. Nasze państwa łączy głębokie zaangażowanie na rzecz globalnej stabilności i bezpieczeństwa – zarówno w wymiarze fizycznym, jak i cyfrowym.

Polska przejawia rosnące zainteresowanie zacieśnianiem współpracy z Kanadyjskimi Siłami Zbrojnymi w dziedzinie obrony cybernetycznej. To zaangażowanie odzwierciedla szersze obawy Polski związane z bezpieczeństwem narodowym i trwającą rosyjską agresją – wyzwaniami, które, jak wiemy, mają wyraźne przełożenie na cyberprzestrzeń. Współpracujemy także intensywnie w ramach forów multilateralnych. Łączy nas wspólne członkostwo w mechanizmach TALON i wspólne zobowiązanie do wspierania cyberodporności Ukrainy wobec uporczywych zagrożeń.

Ale sama technologia nie wystarczy. Aby sprostać rosnącemu zapotrzebowaniu na specjalistów w obszarze cyber, musimy wykorzystać pełen potencjał naszych społeczeństw. W Kanadzie udział kobiet w grupie osób w wieku 16–24 lat, które potrafią programować, wynosi 21 proc. W Polsce to 11 proc. Tymczasem kobiety stanowią zaledwie 21 proc. kanadyjskiej kadry w cyberbezpieczeństwie. To liczba, którą musimy zdecydowanie poprawić. Właśnie dlatego inicjatywy takie jak dzisiejsza mają ogromne znaczenie.

Mam nadzieję, że historie finalistek konkursu zainspirują kolejne kobiety do podejmowania kariery w cyberbezpieczeństwie oraz że powstałe przy tej okazji więzi zaowocują nowymi pomysłami i współpracą.

RISING STAR IN CYBERSECURITY

3 MIEJSCE

MONIKA LEWANDOWSKA

BANK BPS

// Co w pani życiu zmieniło uczestnictwo w konkursie Rising Star in Cybersecurity, a szczególnie zdobycie wyróżnienia i nagrody publiczności?

Uczestnictwo w konkursie Rising Star in Cybersecurity napełniło mnie motywacją do dalszego rozwoju w obszarze cyberbezpieczeństwa. Zdobycie 3. miejsca oraz Nagrody Publiczności utwierdziło mnie w przekonaniu, że jestem we właściwym miejscu – że moje zaangażowanie, pasja i ciężka praca są zauważane i doceniane. Voucher na egzamin certyfikacyjny i członkostwo w ISACA – otwierają przede mną nowe perspektywy i kompetencje, które pozwalają myśleć o bardziej strategicznych rolach w branży.

Ponadto, wystąpienie podczas gali uświadomiło mi, jak ważne jest dzielenie się swoimi osiągnięciami. Ogromną wartością też było dla mnie poznanie ekspertów z branży. Współpraca i wymiana doświadczeń są tym, co najmocniej wspiera rozwój w cyberbezpieczeństwie.

// Czy cyberbezpieczeństwo było jedynym obszarem, który rozpatrywała pani planując edukację i karierę zawodową? Co zdecydowało, że ostatecznie wybrała pani ten kierunek studiów?

Zawsze miałam ścisły umysł i wiedziałam, że chcę rozwijać się na Politechnice Warszawskiej. W roku, w którym aplikowałam, pojawił się tam nowy kierunek – Cyberbezpieczeństwo. Z ciekawości zaczęłam o nim czytać i szybko poczułam, że to ścieżka, która łączy moje zainteresowania i naturalne kompetencje. Postanowiłam spróbować i już po pierwszych semestrach wiedziałam, że to była dobra decyzja.

Cyberbezpieczeństwo to dynamiczna branża, pełna wyzwań i nieustannego rozwoju wymaga odpowiedzialności i krytycznego myślenia. Pozwala tworzyć i wdrażać rozwiązania, które realnie chronią i wspierają ludzi oraz organizacje, co daje największą satysfakcję.

// Z jakim przyjęciem w podmiotach zrzeszonych w sieci banków spółdzielczych spotkało się wprowadzone przez panią rozwiązanie?

Przyjęcie rozwiązania było bardzo pozytywne. Większość zrzeszonych banków sprawnie podjęła się instalacji i szybko zaczęto dostrzegać korzyści z wdrożenia. Wyniki potwierdzają skuteczność systemu, który aktywnie wykrywa zagrożenia i blokuje niepożądane oprogramowanie, realnie wzmacniając cyfrową odporność banków.

Monika Lewandowska

Inżynier cyberbezpieczeństwa z ponadtrzyletnim doświadczeniem. Ścieżkę zawodową rozpoczynała w bankowym zespole SOC, gdzie zajmowała się monitorowaniem cyberzagrożeń, analizą incydentów i threat huntingiem. Karierę w roli analityka bezpieczeństwa IT kontynuowała w firmie usługowej, gdzie miała okazję poznać różne technologie i poziomy dojrzałości firm w kontekście podejścia do cyberbezpieczeństwa. Obecnie pracuje w Banku Polskiej Spółdzielczości w zespole Analiz Cyberbezpieczeństwa (Wydział SOC), gdzie wspiera ponad 300 zrzeszonych banków spółdzielczych w obszarze bezpieczeństwa IT.

Ogromną wartością jest też centralizacja i efekt współdziałania w zrzeszeniu. Zagrożenie wykryte w jednym banku dzięki temu może szybciej zostać zidentyfikowane również w pozostałych. To daje poziom ochrony, który trudno byłoby osiągnąć, gdyby każdy podmiot korzystał wyłącznie z własnego, niezależnego systemu.

// Jak wygląda codzienne zarządzanie / sterowanie EDR-em? Jakie plany na dalszy rozwój platformy?

Codzienne zarządzanie EDR-em polega na bieżącej analizie i obsłudze zagrożeń oraz alarmów generowanych przez system. Zadania te realizujemy jako Zrzeszeniowy Zespół SOC BPS – rozwiązanie łączy więc technologię, kompetencje i wsparcie specjalistów zajmujących się incydentami bezpieczeństwa. Na co dzień śledzimy również nowe funkcje i rekomendacje producenta. Regularnie aktualizujemy system oraz dbamy o jego optymalną konfigurację i poprawne działania administratorów.

System jest stale rozwijany – budujemy nowe reguły detekcyjne i korelacyjne, reagując na aktualne doniesienia z branży, nowe techniki ataków oraz nasze własne obserwacje i analizy.

Planujemy jeszcze bardziej zwiększyć skuteczność detekcji, poprzez tworzenie nowych re-

MONIKA LEWANDOWSKA

BANK BPS

guł dopasowanych do specyfiki banków spółdzielczych. Chcemy też zintegrować system z innymi narzędziami, aby usprawnić analizę i obsługę zdarzeń.

// W trakcie gali konkursowej powiedziała pani, że cyberbezpieczeństwo to branża dla kobiet, które lubią wyzwania. Dlaczego?

Cyberbezpieczeństwo to branża pełna wyzwań – wymaga odwagi, determinacji, analitycznego myślenia, otwartości i ciągłego poszerzania kompetencji. Atakujący cały czas szukają nowych metod, a naszą rolą jest być zawsze o krok przed nimi. Nieustannie pojawiają się nowe zagrożenia i scenariusze, które wymagają szybkiej reakcji. Równie szybko rozwijają się narzędzia, z których korzystamy – dlatego niezbędne jest ciągłe uczenie się i doskonalenie, co sprawia, że w tej pracy nie ma miejsca na rutynę.

Dlatego uważam, że to idealna przestrzeń dla kobiet, które lubią wyzwania. Największą satysfakcję daje poczucie sprawczości – moment, w którym widzimy, że nasze działania realnie podnoszą poziom bezpieczeństwa i chronią innych. To poczucie wynagradza włożony wysiłek.

// W czym, w pani ocenie, tkwi podstawowa przyczyna niewystarczającej reprezentacji kobiet w branży IT?

Myślę, że to kwestia utrwalonych przekonań, że kierunki techniczne są domeną mężczyzn. Tymczasem w branży IT płeć nie stanowi żadnej przeszkody i nie ogranicza naszych możliwości. Tutaj najważniejsze są kompetencje, wiedza i zaangażowanie. Cyberbezpieczeństwo, opiera się na kompetencjach intelektualnych, które wiele kobiet posiada i rozwija. Potwierdzają to statystyki – obecnie w Polsce to kobiety stanowią większą część absolwentów studiów wyższych.

// Czy widzi się pani w roli mentorki dla innych kobiet, przyszłych adeptek informatyki lub cyberbezpieczeństwa?

Chciałabym wspierać kobiety, które wchodzą do branży IT i cyberbezpieczeństwa. Wierzę, że współpracując z mężczyznami mamy ogromny potencjał, by zmieniać tę branżę, wyznaczać nowe kierunki i odgrywać istotną rolę w budowaniu bezpiecznej cyfrowej przyszłości.

Projekt zgłoszony do Rising Star in Cybersecurity Zrzeszeniowy EDR

Banki spółdzielcze zrzeszone w Banku Polskiej Spółdzielczości, mimo że działają lokalnie i są mniejsze niż duże instytucje finansowe, podlegają tym samym zagrożeniom i regulacjom, takim jak rozporządzenie DORA. Wyzwanie polega na tym, że koszty zaawansowanych systemów bezpieczeństwa są dla nich dużym obciążeniem, a każdy z banków posiadał wcześniej własne, w różnym stopniu zaawansowane rozwiązania antywirusowe.

Odpowiedzią na ten problem było wdrożenie zrzeszeniowego systemu Endpoint Detection & Response. EDR pozwala centralnie zarządzać bezpieczeństwem wszystkich instytucji zrzeszonych. Projekt objął 307 banków spółdzielczych oraz Bank BPS, co oznaczało instalację agentów na blisko 20 tysiącach urządzeń.

Zrzeszeniowy EDR działa jak Google Maps – zbiera dane telemetryczne od banków, analizuje je w czasie rzeczywistym i pozwala reagować szybciej i skuteczniej. Dzięki centralizacji dział Security Operations Center zyskuje pełen obraz sytuacji, może tworzyć dedykowane reguły dopasowane do specyfiki banków spółdzielczych, a także szybciej reagować na nowe zagrożenia.

Projekt był realizowany w bardzo wymagających warunkach: skala wdrożenia obejmowała setki instytucji i tysiące urządzeń, czas był ograniczony (aby zdążyć przed wejściem w życie regulacji DORA) a różnorodność środowisk IT w bankach wymagała szczególnej ostrożności, by uniknąć konfliktów z istniejącym oprogramowaniem. Kluczowe znaczenie miała ciągłość działania systemów bankowych – instalacja nie mogła wpływać na wydajność i stabilność pracy.

Dzięki sprawnej współpracy i wsparciu technicznemu, w ciągu trzech miesięcy system został wdrożony we wszystkich zrzeszonych instytucjach. Obecnie zrzeszeniowy EDR stanowi serce SOC-u, a jego funkcje wykraczają poza ochronę przed atakami – to także główne źródło danych telemetrycznych, narzędzie do reagowania na incydenty oraz fundament dalszego rozwoju cyfrowej odporności banków spółdzielczych.

BNP PARIBAS

KOMENTARZ EKSPERCKI

Iwona Dobrzańska
Lead Security Officer,
BNP Paribas Bank Polska S.A.

Kobiety w dziedzinie IT odgrywają niezwykle istotną rolę, chociaż przyjęło się, że jest to typowo męski obszar. Wynika to z trwałego stereotypu, że zawody techniczne są domeną mężczyzn, co przekłada się na wybory edukacyjne kobiet. Jak dowodzą statystyki publikowane przez „Perspektywy", trend na uczelniach technicznych w ciągu ostatniej dekady pokazuje stabilny, lecz niski udział kobiet (około 33-34 proc.), z niewielkimi wzrostami na kierunkach informatycznych i innych nowych technologiach, które osiągnęły około 16-20 proc. udziału kobiet w latach 2023/2024, choć nadal pozostają zdominowane przez mężczyzn.

„Odczarowanie" rynku IT jako stereotypowo męskiego, by przyciągnąć kobiety do branży IT, jest możliwe poprzez promowanie edukacji technicznej, tworzenie programów monitoringowych, eliminowanie nierówności płacowych, budowanie kultury organizacyjnej kładącej nacisk na różnorodność i zmiany w stereotypach o roli kobiet w technologii. Promowanie edukacji technicznej powinno być realizowane poprzez zapewnianie i wspieranie w dostępie do kursów IT. Ważne, aby program edukacji obejmował również osoby z wykształceniem humanistycznym, które chcą się przebranżowić w danym momencie swojej kariery zawodowej.

W sektorze IT brak konkretnych, dedykowanych obszarów IT dla kobiet. W tej branży, podobnie jak w innych, kluczowe są również umiejętności miękkie. Warto pamiętać, że branża IT jest dynamiczna i wszechstronna, oferując wiele ścieżek kariery. Nie ogranicza się ona do jednego typu stanowiska, co pozwala na znalezienie miejsca dla kobiet z różnymi umiejętnościami i doświadczeniem.

Karolina Czwarno-Kos
Dyrektorka Biura Zapobiegania Oszustwom Cyfrowym i Komunikacji Cyberbezpieczeństwa,
BNP Paribas Bank Polska S.A.

Obecnie kobiety stanowią około 25 proc. specjalistów w cyberbezpieczeństwie, podczas gdy jeszcze dekadę temu ich udział wynosił zaledwie 10 proc. Choć jest to znaczący postęp, wciąż pozostajemy daleko od parytetu. Dlatego z inicjatyw wspierających kobiety w IT, takich jak BNP Paribas Women Up czy Rising Star in Cybersecurity rynek może wyciągnąć wiele ważnych lekcji. Takie programy pokazują, że warto aktywnie inwestować w talenty – kobiety nadal stanowią ogromny, niewykorzystany potencjał. Jeszcze niedawno źródła problemu szukano głównie na etapie studiów technicznych, gdzie przewaga mężczyzn nad kobietami jest wyraźna. Dziś jednak coraz częściej do świata cyberbezpieczeństwa trafiają osoby kierujące się pasją i zainteresowaniami, co otwiera przestrzeń dla większej różnorodności.

Widoczność i wyróżnienia – jak nagrody Rising Star – przełamują stereotypy i zwiększają obecność kobiet w rolach eksperckich i przywódczych. Z kolei programy mentoringowe i edukacyjne, jak np. BNP Paribas Women Up, realnie podnoszą kompetencje, a jednocześnie poprawiają retencję pracowników – co potwierdzają dane z organizacji, które takie programy wdrożyły. Badania jednoznacznie pokazują, że zespoły zróżnicowane pod względem płci wzmacniają zdolność firmy do innowacji oraz zwiększają jej atrakcyjność dla klientów i inwestorów. Jak wynika z raportu Grant Thornton „Women in Business 2025: Impacting the missed generation", firmy, które opóźniają świadome działania na rzecz parytetu płci, nie tylko zostają w tyle w zakresie różnorodności, ale także ryzykują utratę przewagi konkurencyjnej i ograniczają swój potencjał wzrostu.

RISING STAR IN CYBERSECURITY

WYRÓŻNIENIE

ANNA KROKER

EY

// Od ochrony zdrowia do ochrony danych i systemów – co było najtrudniejsze w pani zawodowej transformacji?

Przejście z ochrony zdrowia do cyberbezpieczeństwa było jak skok na głęboką wodę. Trudne było zrozumienie zupełnie nowych terminów i technologii, ale najtrudniejsze to podjęcie tej decyzji do działania i zmiany – „robię to!" Oczywiście dodatkowe studia na kierunku Health Informatics były niezwykle pomocne w tej transformacji, łączyły oba kierunki jak taki most pomiędzy dwoma wyspami. To była spora zmiana, ale z czasem zaczęłam dostrzegać, jak te dwa światy się przenikają – w końcu chodzi o bezpieczeństwo, niezależnie od kontekstu.

// Co sprawiło, że mimo początkowych obaw zdecydowała się pani wejść do świata cyberbezpieczeństwa?

Miałam swoje obawy, ponieważ cyberbezpieczeństwo to z pewnością nie jest najłatwiejsza dziedzina. Jednak zafascynowało mnie, jak dynamicznie się rozwija i jak kluczowe jest w dzisiejszym świecie. Zrozumiałam, że mogę wykorzystać swoje umiejętności i doświadczenie, aby pomóc innym w bezpiecznym korzystaniu z technologii. Mimo zdecydowanych różnic w wykonywanych zadaniach moje podejście do pracy pozostało niezmienne. Umiejętności analityczne oraz zdolność do komunikacji z ludźmi są cenne w każdej branży.

Cyberbezpieczeństwo to niezwykle różnorodna dziedzina; odkryłam, że kryje w sobie znacznie więcej tematów niż tylko pentesty. Znalazłam swoje miejsce w tej branży. Jednak muszę podkreślić, że to ciągła nauka i nieustanne podnoszenie kwalifikacji. Zdecydowanie trzeba chcieć tej zmiany i być gotowym na nowe wyzwania.

// Podkreśla pani, że zarządzanie ryzykiem stron trzecich to nie dodatek, ale fundament cyberbezpieczeństwa. Jakie największe wyzwania widzi pani dziś w tym obszarze i jakie dobre praktyki warto wdrażać w organizacjach?

Zarządzanie ryzykiem stron trzecich to niezwykle istotny, a często niedoceniany temat. Największym wyzwaniem w tej dziedzinie jest brak przejrzystości w relacjach z dostawcami, co często wynika z niejasno określonych ról w organizacji oraz rozproszonego lub wręcz nieistniejącego procesu. Zarządzanie ryzykiem stron trzecich powinno być integralnym elementem onboardingu dostawcy. To nie tylko zadanie działu zakupów, ale także osobnego zespołu, który dokładnie przeanalizuje dostawcę pod ką-

tem bezpieczeństwa, dostępu do danych oraz systemów organizacji.

Ważne jest, aby przeprowadzać szczegółowe kontrole dokumentów, certyfikatów i raportów, a także realizować oceny ryzyka. Kluczowe są rozmowy z dostawcą, zespołem biznesowym, działem IT oraz innymi interesariuszami. Dodatkowym wyzwaniem są nowe regulacje, takie jak DORA czy NIS2, które wymagają dostosowania już istniejących procesów.

Niestety, w wielu organizacjach brakuje świadomości na temat tego procesu. Dlatego tak istotne jest ciągłe podnoszenie świadomości wśród pracowników dotyczącej współpracy z dostawcami oraz ich dostępu do danych i systemów. Ryzyko, jakie niosą za sobą takie dostępy, może prowadzić nie tylko do strat wizerunkowych, ale także do ogromnych strat finansowych.

A przecież można tego uniknąć. Na rynku dostępnych jest wielu dostawców, którzy stosują dobre praktyki bezpieczeństwa i posiadają odpowiednie certyfikaty. Warto również inwestować w edukację zespołów na temat ryzyk związanych z dostawcami oraz wprowadzać jasne procedury reagowania na incydenty. Kluczowa jest także komunikacja i współpraca między zespołami, które pozwalają na skuteczniejsze zarządzanie ryzykiem.

Anna Kroker

Posiada doświadczenie w zakresie zarządzania ryzykiem związanym ze stronami trzecimi (Third-Party Risk Management, TPRM). Skupia się na identyfikacji, ocenie i minimalizacji ryzyk wynikających z relacji z dostawcami, a także zarządzaniu ryzykiem aplikacji. Aktywnie uczestniczyła w projektach wdrażających procesy TPRM i działania operacyjne dla globalnych firm, opracowując strategie kładące nacisk na bezpieczeństwo informacji i zgodność z regulacjami. Korzysta z narzędzi takich jak ServiceNow, AuditBoard i Asana, efektywnie zarządzając relacjami z interesariuszami oraz prowadząc szkolenia dla zespołu. Interesuje się medycyną, koszykówką i kulturą Skandynawii, a w wolnym czasie chętnie czyta książki.

ANNA KROKER

BANK BPS

// Jak pani zdaniem kobiety mogą wnosić do branży cyber inne podejście do przywództwa i współpracy zespołowej?

Kobiety często wnoszą do zespołów empatię i umiejętność słuchania, co jest niezwykle cenne. Współpraca oraz zrozumienie potrzeb innych członków zespołu prowadzą do lepszych rozwiązań. Kobiety mogą również inspirować do bardziej zrównoważonego podejścia do przywództwa, które uwzględnia różnorodność i różne perspektywy. To właśnie ta perspektywa jest kluczowa. Obecność kobiet w zespole pozwala dostrzegać pośrednie, a czasem nawet inne sposoby usuwania problemów, wychodzić poza rozwiązania zero-jedynkowe. Dzięki temu możemy podejść do wyzwań w sposób bardziej kreatywny i kompleksowy, co z pewnością przynosi korzyści całej organizacji.

// Dlaczego, pani zdaniem, obecność kobiet w cyber jest tak ważna? Jakie unikatowe perspektywy i umiejętności mogą one wnosić?

Różnorodność w zespole sprzyja podejmowaniu lepszych decyzji i stymuluje innowacje. Kobiety często wnoszą odmienne doświadczenia i perspektywy, co pozwala na tworzenie bardziej kompleksowych strategii bezpieczeństwa. Ich umiejętności w zakresie komunikacji i współpracy są nieocenione w budowaniu efektywnych zespołów.

Co więcej, kobiety w technicznych dziedzinach stanowią inspirację dla innych kobiet. Widząc, że jedna z nich odnosi sukcesy, wiele kobiet myśli: „Skoro ona może, to dlaczego ja miałabym nie spróbować?”. Taki rozwój zachęca kolejne kobiety do podjęcia wyzwań, co prowadzi do coraz większej reprezentacji kobiet w zespołach w organizacjach. Osobiście cieszę się, że w moim otoczeniu jest więcej kobiet niż mężczyzn, co tylko potwierdza, że różnorodność jest kluczem do sukcesu w tej branży.

// Co poradziłaby pani młodym kobietom, które dopiero wchodzą na rynek pracy i myślą o karierze w cyberbezpieczeństwie, ale zniechęca je stereotyp „męskiej branży”?

Przede wszystkim, nie dajcie się zniechęcić! Cyberbezpieczeństwo to dziedzina, która potrzebuje różnorodnych talentów i perspektyw. Stereotypy to jedynie przeszkody, które można pokonać. Warto szukać mentorek, które mogą wspierać was w rozwoju kariery, a także angażować się w społeczności, które promują kobiety w technologii.

Chciałabym również nawiązać do tego, co mówiłam w trakcie prezentacji na gali konkursowej: mówcie „tak” okazjom i nie bójcie się spróbować! To właśnie zmiana i transformacja mogą okazać się punktem zwrotnym w waszym życiu. Niech odwaga do działania prowadzi was ku nowym możliwościom!

Projekt zgłoszony do Rising Star in Cybersecurity
Zarządzanie ryzykiem stron trzecich

Współczesne przedsiębiorstwa funkcjonują w złożonych ekosystemach, opartych na współpracy z wieloma partnerami zewnętrznymi – od dostawców usług IT, przez firmy zarządzające danymi, aż po partnerów technologicznych. Każdy z tych podmiotów może stać się potencjalnym wektorem ataku.

Rolą procesów Third-Party Risk Management jest więc monitorowanie, weryfikacja i kontrola zgodności dostawców z przyjętymi standardami bezpieczeństwa. W praktyce oznacza to nie tylko ocenę ryzyka, ale także budowanie przejrzystych procesów, które pozwalają skutecznie zarządzać całym cyklem życia dostawcy – od pierwszej weryfikacji po bieżący nadzór.

Anna Kroker z sukcesem przekształciła procesy TPRM u jednego z kluczowych klientów EY, przechodząc z manualnego na automatyczne zarządzanie, wprowadzając transparentny podział odpowiedzialności i zdefiniowany cykl zarządzania ryzykiem. Efektem było skalowalne, przejrzyste i efektywne podejście do zarządzania ryzykiem stron trzecich, które ogranicza ryzyko operacyjne i zwiększa dojrzałość organizacji w obszarze bezpieczeństwa.

W trakcie transformacji kluczowe znaczenie miała także współpraca i przywództwo: konsultacje z regionalnymi CISO i liderami technicznymi z różnych krajów, a także mentoring i wsparcie zespołu. Dzięki temu zmiana nie była wyłącznie techniczna, lecz również organizacyjna – TPRM stał się realnym narzędziem podnoszącym odporność całej firmy.

RISING STAR
IN CYBERSECURITY

JURY 4. EDYCJI KONKURSU

MAŁGORZATA BJØRUM
CISO, POLSKIE PORTY LOTNICZE S.A.

ROBERT PAJĄK
CEMA CUSTOMER SECURITY OFFICER & CHIEF SECURITY ADVISOR, MICROSOFT

IWONA DOBRZAŃSKA
LEAD SECURITY OFFICER, BNP PARIBAS BANK POLSKA

EWA PIŁAT
CHIEF INFORMATION SECURITY OFFICER, IATA

AGNIESZKA GAWĘCKA-KOPYTKO
KIEROWNIK ZESPOŁU ZARZĄDZANIA OPERACYJNEGO I CIĄGŁOŚCI DZIAŁANIA, TAURON

MAGDALENA SKORUPA
PRESIDENT, ISC2 POLAND CHAPTER

MONIKA GLIWKA
ZWYCIĘŻCZYNI KONKURSU RISING STAR IN CYBERSECURITY 2024, MINISTERSTWO CYFRYZACJI

ALICJA SKRABURSKA
HEAD OF CYBERSECURITY ENTERPRISE TECHNOLOGY, HSBC

MAGDALENA JAKIMIUK
HEAD OF GLOBAL CYBER THREAT MANAGEMENT, DB SCHENKER

MONIKA TOŚTA
INSPEKTOR OCHRONY DANYCH OSOBOWYCH, KOLPORTER

AGATA KULAS
HEAD OF DATA ASSESSMENTS AND PROCESSING ACTIVITIES, CHIEF DATA OFFICE, STANDARD CHARTERED BANK

AGNIESZKA ULANOWSKA
DYREKTOR DZIAŁU NADZORU WEWNĘTRZNEGO I BEZPIECZEŃSTWA IT, NOBLE FUNDS TFI, ISACA WARSAW CHAPTER

ANETA LEGENZA
HEAD OF CYBERDEFENSE OPERATIONS, BANK MILLENNIUM

ALINA ZAJĄC
IT SECURITY MANAGER/ HEAD OF CERT PL, E.ON

RISING STAR IN CYBERSECURITY

WYRÓŻNIENIE

JULIA LISOWSKA-WENTA

BNP PARIBAS POLSKA

// Jakie momenty dały pani największą satysfakcję w trakcie realizacji projektu?

Największą satysfakcję dawał mi bezpośredni kontakt z seniorami. Ogromną radością było też usłyszeć, że dzięki szkoleniom seniorzy czują się spokojniejsi, a nawet potrafią ostrzec swoich bliskich przed potencjalnym zagrożeniem. To pokazuje, że działania edukacyjne naprawdę mają wpływ na codzienne życie.

// Jak pani ocenia rolę i wpływ kobiet w obszarze security – co wnoszą i jak zmieniają perspektywę postrzegania problematyki bezpieczeństwa?

Kobiety wnoszą do cyberbezpieczeństwa unikalną perspektywę – zwracają większą uwagę na czynnik ludzki, komunikację i praktyczne potrzeby użytkowników, co uzupełnia mocno techniczne spojrzenie, które często dominuje w tej branży. To nie znaczy, że mężczyźni nie

Kobiety wnoszą do cyberbezpieczeństwa unikalną perspektywę – zwracają większą uwagę na czynnik ludzki, komunikację i praktyczne potrzeby użytkowników, co uzupełnia mocno techniczne spojrzenie, które często dominuje w tej branży. To nie znaczy, że mężczyźni nie mają podobnych kompetencji – wręcz przeciwnie, wierzę, że różnorodność zespołów, płci i doświadczeń zawodowych sprawia, że rozwiązania są pełniejsze i bardziej skuteczne.

Julia Lisowska-Wenta

Od ponad 10 lat pracuje w obszarze bankowości i związana jest ze sferą cyberbezpieczeństwa. Specjalistka w zakresie działań antyfraudowych oraz edukacji o bezpieczeństwie. Absolwentka studiów podyplomowych w zakresie zapobiegania, wykrywania i zwalczania cyberprzestępstw popełnianych na szkodę banków oraz ich klientów w Wyższej Szkole Policji w Szczytnie.

mają podobnych kompetencji – wręcz przeciwnie, wierzę, że różnorodność zespołów, płci i doświadczeń zawodowych sprawia, że rozwiązania są pełniejsze i bardziej skuteczne.

// Czy podczas swojej kariery zawodowej spotkała się pani z barierami związanymi z tym, że cyberbezpieczeństwo to wciąż branża mocno zdominowana przez mężczyzn?

Branża rzeczywiście bywa postrzegana jako bardziej „męska", co czasami powoduje, że kobiety muszą udowadniać swoje kompetencje nieco mocniej. Osobiście staram się traktować to raczej jako wyzwanie niż barierę. Cieszę się, że coraz więcej firm i instytucji otwarcie wspiera kobiety w cyberbezpieczeństwie, bo ta różnorodność wzmacnia cały sektor. Wierzę, że najwięcej możemy osiągnąć wtedy, gdy łączymy perspektywy i doświadczenia – zarówno kobiet, jak i mężczyzn – bo bezpieczeństwo cyfrowe to wspólna sprawa.

// Jakie formy edukacji uważa pani za najbardziej efektywne w budowaniu świadomości cyberzagrożeń?

Najlepiej sprawdza się edukacja praktyczna w postaci warsztatów. Ludzie zapamiętują

JULIA LISOWSKA-WENTA

BNP PARIBAS POLSKA

znacznie więcej, gdy mogą zobaczyć na żywo symulacje ataków niż gdy tylko usłyszą teorię. Kluczowa jest też prostota przekazu – nie każdy musi znać żargon techniczny, ale każdy powinien wiedzieć, jak rozpoznać podejrzany SMS, e-mail czy telefon.

// Jak zwiększać odporność społeczeństwa na manipulację emocjonalną, która często stoi za cyberoszustwami?

Przede wszystkim przez edukację i budowanie nawyku krytycznego myślenia. Cyberoszuści bazują na emocjach – strachu, pośpiechu, dezorientacji. Jeśli nauczymy ludzi, że zawsze warto „dać sobie chwilę", sprawdzić źródło informacji, zadzwonić do banku czy instytucji zamiast ufać temu, co słyszymy w słuchawce lub widzimy w telefonie czy na komputerze – znacząco zwiększamy ich odporność. Ważne jest też oswajanie tego tematu: im więcej mówimy o cyberzagrożeniach w szkołach, na uniwersytetach trzeciego wieku czy w mediach, tym bardziej ten temat przestaje być „niewidzialny". Tylko tak możemy przygotować użytkowników bankowości na zagrożenia pojawiające się wokół nich.

// Jak udział w Rising Star in Cybersecurity wpłynął na pani rozwój zawodowy i projekt? Czy czuje pani, że ten konkurs nie tylko daje narzędzia, ale też wzmacnia widoczność kobiet w świecie cyberbezpieczeństwa i IT?

Udział w konkursie był dla mnie inspirujący – pozwolił nie tylko zaprezentować projekt, ale też poznać osoby, które podobnie jak ja chcą zmieniać świat cyberbezpieczeństwa na lepsze. Jestem przekonana, że inicjatywy takie jak Rising Star in Cybersecurity mają ogromną wartość, bo budują widoczność kobiet i pokazują, jak istotny jest ich wkład. Jednocześnie dostrzegam, że prawdziwą siłę tej branży stanowi różnorodność – otwartość na różne style pracy, doświadczenia i punkty widzenia, niezależnie od płci. To ona sprawia, że wspólnie możemy wypracować jeszcze skuteczniejsze rozwiązania.

Projekt zgłoszony do Rising Star in Cybersecurity
Edukacja seniorów

Julia Lisowska-Wenta od blisko dekady obserwuje i analizuje różne formy przestępczości w bankowości elektronicznej. Na co dzień monitoruje podejrzane transakcje w systemach antyfraudowych, ale równie ważną częścią jej pracy jest edukacja użytkowników, by wiedzieli, jak chronić siebie i swoje finanse.

Z jej obserwacji wynika, że szczególnie narażoną grupą są osoby starsze. To grupa o ogromnym genie zaufania, ale o bardzo zróżnicowanym poziomie znajomości technologii. Niektórzy świetnie radzą sobie w bankowości internetowej, inni nie korzystają z niej wcale – często ich kontami zarządzają bliscy. Tymczasem z badań Warszawskiego Instytutu Bankowości z 2023 r. wynika, że ponad 30 proc. seniorów padło ofiarą oszustów, a jedynie niespełna 30 proc. potrafi zweryfikować tożsamość osoby podającej się za pracownika banku.

Przestępcy najczęściej wykorzystują socjotechnikę – podszywają się pod policjantów, pracowników banków, instytucje publiczne lub oferują fałszywe inwestycje. Coraz częściej oszustwa mają też miejsce w popularnych serwisach ogłoszeniowych, a ogromnym problemem pozostają fałszywe SMS-y i e-maile.

Tak zrodziła się koncepcja projektu edukacyjnego dla seniorów – bezpośrednie spotkania organizowane we współpracy z uniwersytetami trzeciego wieku i kołami emerytów. Projekt pozwala jej łączyć role specjalistki wykorzystującej technologię do ochrony transakcji i edukatorki, która wzmacnia odporność cyfrową poprzez bezpośredni kontakt z ludźmi.

Spotkania są dostosowane do poziomu wiedzy uczestników. Podczas tych wydarzeń ekspertka pokazuje realne przykłady oszustw, tłumaczy je prostym, zrozumiałym językiem i wyjaśnia, czym jest phishing, malware czy socjotechnika. Uczestnicy spotkań mogą dowiedzieć, się jak przestępcy manipulują emocjami, autorytetem czy obietnicą zysku oraz jak odróżniać prawdziwe oferty od fałszywych i jakie funkcje bezpieczeństwa warto włączyć w bankowości elektronicznej.

Cyber Women Community

ZAPRASZAMY NA NOWĄ EDYCJĘ 2026

RISING STAR IN CYBERSECURITY

IV EDYCJA KONKURSU

ZAPRASZAJĄ:

JURY, ORGANIZATORZY I PARTNERZY KONKURSU.

Cyber Women Community

SPOŁECZNOŚĆ KOBIET Z BRANŻY CYBERSECURITY

cyberwomen.eu

CYBER WOMEN COMMUNITY TO SPOŁECZNOŚĆ KOBIET SKUPIONYCH WOKÓŁ TEMATU CYBERBEZPIECZEŃSTWA. ŁĄCZYMY EKSPERTKI Z PANIAMI, KTÓRE DOPIERO ROZPOCZYNAJĄ SWOJĄ KARIERĘ W CYBERSECURITY.

Szkolimy, tłumaczymy i pokazujemy jak fascynującą branżą jest cyberbezpieczeństwo i że jest w niej miejsce i mnóstwo możliwości - dla kobiet!

Spotykamy się na warsztatach i konferencjach, bierzemy udział w akcjach charytatywnych oraz dniach kariery na uczelniach. Nasze ekspertki są wykładowcami na znanych uczelniach m.in. Akademii Leona Koźmińskiego.

Dołącz i sprawdź, ile możemy zdziałać razem!

3 260	**ponad 300**	**6**	**26**
OBSERWUJĄCYCH	CZŁONKIŃ SPOŁECZNOŚCI	SPOTKAŃ W ROKU	W RADZIE I KLUBIE EKSPERTEK

ZRÓBMY RAZEM COŚ WSPANIAŁEGO

EVENTION
CZAS ZAANGAŻOWANY

Evention to firma z 12-letnią historią, znana z tworzenia programów wymiany wiedzy i rozwoju społeczności (poprzez organizację regularnych spotkań i konferencji) dla dyrektorów, menedżerów i ekspertów odpowiedzialnych za obszar technologii, bezpieczeństwa i cyfryzacji. Firma Evention realizuje od lat uznane na rynku konferencje branżowe, cykliczne spotkania dedykowane dla managerów oraz publikacje specjalne (raporty, projekty badawcze). Robimy w Evention rzeczy wyjątkowe i niepowtarzalne – a w swoim obszarze rynku jesteśmy liderem. Potwierdzeniem tego są zdobyte wyróżnienia i nagrody: Gazeli Biznesu 2023 oraz Diamenty Forbesa 2023/2024/2025. To prestiżowe rankingi pokazujące najbardziej dynamicznie rozwijające się firmy MŚP, gotowe sprostać współczesnym wyzwaniom rynku. Więcej o nas na stronie: **www.evention.pl**.