Katarzyna Grabowska
NASK

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

dr inż. Anna Felkner
NASK

Rozmowa z dr inż. Anną Felkner, Dyrektor Pionu Badań i Rozwoju Cyberbezpieczeństwa NASK.

KG: Jak postrzegasz rolę kobiet w nauce w obszarze związanym z cyberbezpieczeństwem?

AF: Rola kobiet w nauce, zwłaszcza w cyberbezpieczeństwie, jest coraz bardziej zauważalna i potrzebna. Choć wciąż jesteśmy w mniejszości, to nasza obecność ma ogromne znaczenie - łamiemy stereotypy i pokazujemy, że umiejętności badawcze, analityczne czy organizacyjne nie są powiązane z płcią. Podczas mojej pracy w projektach takich jak VARIoT (Vulnerability and Attack Repository for IoT) czy AIPITCH (AI-Powered Innovative Toolkit for Cybersecurity Hubs), miałam okazję zaobserwować, jak różnorodność w zespołach przekłada się na skuteczność i innowacyjność rozwiązań. Cyberbezpieczeństwo wymaga spojrzenia z wielu stron - a kobiety wnoszą nie tylko interdyscyplinarność, ale także unikalną wrażliwość, dużą determinację oraz nieoczywiste podejście do rozwiązywania problemów. Fundamentem odporności i przydatności systemów jest właśnie różnorodność punktów widzenia. Cennym uzupełnieniem tej perspektywy jest dla mnie aktualnie możliwość uczestnictwa jako mentorka w programie MAK prowadzonym przez NASK, skupiającym się na wymianie doświadczeń, rozwijaniu kompetencji i budowaniu wzajemnego wsparcia wśród kobiet obecnych w nowych technologiach. Udział w nim daje nie tylko szansę dzielenia się wiedzą, ale także uczy mnie nowych ról oraz pokazuje, jaką energię wnoszą

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

kobiety rozpoczynające karierę w cyberbezpieczeństwie.

KG: Co skłoniło Cię do wyboru tej ścieżki zawodowej?

AF: Istotnym aspektem mojej pracy zawodowej jest jej praktyczna wartość oraz możliwość wywierania realnego wpływu - zarówno na ludzi, jak i na projekty, w które się angażuję. Początkowo droga naukowa wydawała mi się naturalna, ale szybko zrozumiałam, że potrzebuję też praktycznych działań.

Cyberbezpieczeństwo to nie tylko technologia, ale także ludzie i zaufanie. Ta interdyscyplinarność - połączenie zagadnień technicznych, organizacyjnych i społecznych - sprawiła, że poczułam, iż mogę łączyć zainteresowanie nauką z realnym wpływem na bezpieczeństwo społeczeństwa. Ogromną satysfakcję daje mi łączenie wiedzy i działalności naukowej z praktyką, z wdrożeniami i współpracą z różnorodnymi zespołami. Doceniam też szansę na ciągłe uczenie się, bo w tej dziedzinie nieustannie pojawiają się nowe wyzwania i obszary do eksploracji - od kwestii technicznych aż po komunikację i edukację użytkowników.

KG: Z jakimi największymi wyzwaniami spotkałaś się podczas koordynowania prac w międzynarodowych projektach?

AF: Wyzwań jest wiele i zdecydowanie stanowią najciekawszy, choć czasem najtrudniejszy, element tej pracy. Po pierwsze - różnice kulturowe i sposoby zarządzania: każda firma, instytucja czy zespół ma inną dynamikę, własne priorytety i organizację pracy. Trzeba odnaleźć wspólny język - nie tylko dosłownie, ale też w sensie wartości czy oczekiwań.

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

W projekcie EUNITY, gdzie współpracowałam z instytucjami japońskimi, różnice w sposobie komunikacji i budowania relacji były szczególnie odczuwalne - tam cierpliwość i wzajemne zaufanie były kluczem do powodzenia. Praca z zespołami międzynarodowymi nauczyła mnie elastyczności i pokory - wartości, które uważam za nieodzowne w dzisiejszym, złożonym środowisku pracy.

Po drugie - motywacja zespołów. Wyzwaniem jest nie tyle narzucenie zadania, co przekonanie partnerów, że realizowany przez nas projekt jest niezwykle ważny, że przyczyni się do większego bezpieczeństwa. Często osoby zaangażowane mają również inne zobowiązania, własne projekty. Dlatego kluczowe jest, by z jednej strony zbudować osobiste relacje, a z drugiej, stworzyć poczucie wspólnej misji.

Nierzadko pracuję z bardzo doświadczonymi specjalistami, którzy świetnie znają uwarunkowania, potrzeby i dynamikę funkcjonowania swojego otoczenia zawodowego. Jednak aby rzeczywiście móc ruszyć do przodu, moim zadaniem jako liderki jest nie tylko im zaufać, lecz także zadbać o to, by czuli się częścią czegoś większego. Liczy się transparentna komunikacja, otwartość na rozmowę, cierpliwość, docenianie drobiazgów i wspólne świętowanie nawet tych małych sukcesów. To daje zespołowi energię do działania nawet wtedy, gdy pojawiają się trudności lub napięte terminy.

KG: Czym dla Ciebie jest podnoszenie świadomości cyberbezpieczeństwa?

AF: To edukacja i budowanie odpowiedzialności - zarówno wśród użytkowników,

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

jak i w organizacjach. Nie chodzi tylko o użytkowników końcowych, ale też decydentów i liderów, bo od nich zależy kultura bezpieczeństwa w organizacjach. Można stworzyć najbardziej zaawansowany system bezpieczeństwa, ale jeśli człowiek popełni błąd, cała ochrona przestaje działać. Dlatego świadomość to fundament - uczymy ludzi nie tylko jak się chronić, ale też dlaczego to jest tak bardzo ważne. Sama technologia bez edukacji i odpowiedzialności społecznej jest niewystarczająca. W ramach prac w projekcie VARIoT stworzyliśmy bazę informacji o podatnościach i eksploitach w Internecie Rzeczy. Nasze działania promocyjne projektu przyczyniły się do zainteresowania społeczeństwa nie tylko samą bazą, ale też, a może nawet przede wszystkim, zagrożeniami związanymi z posiadaniem podatnych urządzeń IoT i sposobami ich zabezpieczania. Z mojej perspektywy jest niezwykle budujące to kiedy użytkownicy urządzeń sami z siebie interesują się ich bezpieczeństwem ☺

KG: Jak na przestrzeni lat zmienił się charakter zagrożeń w kontekście systemów i urządzeń i jakie czynniki utrudniają skuteczne wzmacnianie ich odporności?

AF: Kiedyś mieliśmy do czynienia głównie z wirusami i indywidualnymi atakami, teraz są to całe zorganizowane grupy cyberprzestępcze, a nawet działania państw. Ataki stały się bardziej wyrafinowane: wymierzone w infrastrukturę krytyczną, łańcuchy dostaw, urządzenia IoT czy systemy oparte na sztucznej inteligencji. Duże wyzwanie stanowi obecnie automatyzacja ataków przy wykorzystaniu narzędzi opartych o AI oraz złożone kampanie phishingowe

przeprowadzane z użyciem deepfake'ów. Problemem pozostaje również ogromna liczba urządzeń podłączonych do sieci, które często nie były projektowane z myślą o bezpieczeństwie. Dodatkowymi barierami są szybkie tempo rozwoju technologii, brak jednolitych regulacji, a także niedobór doświadczonych specjalistów, przez co skuteczna ochrona wymaga ciągłego podnoszenia kompetencji i wymiany wiedzy w skali globalnej.

KG: Jak widzisz przyszłość roli nauki w rozwoju cyberbezpieczeństwa (w kontekście wyzwań cyfrowych)?

AF: Nauka będzie pełnić absolutnie kluczową rolę, żeby przewidywać nowe zagrożenia i oferować innowacyjne rozwiązania, zanim pojawią się realne problemy.

Rośnie znaczenie współpracy pomiędzy nauką a przemysłem - żeby badania nie zostawały tylko w laboratoriach. Potrzebujemy badań nie tylko nad nowymi algorytmami, kryptografią postkwantową czy bezpieczeństwem sztucznej inteligencji, ale także nad aspektem społecznym i psychologicznym cyberbezpieczeństwa. Z jednej strony naukowcy będą musieli odpowiadać na bieżące potrzeby przemysłu i państw, z drugiej - patrzeć w przyszłość i przygotowywać rozwiązania na zagrożenia, które dopiero się wyłonią. Widzę też rosnące znaczenie multidyscyplinarnych zespołów - łączących informatyków, analityków, socjologów, psychologów i prawników - żaden z tych obszarów nie wyczerpuje tematu bezpieczeństwa samodzielnie. Dostrzegam też ogromną rolę badań stosowanych, które - jak w NASK - łączą teorię z praktyką i przekładają

się na realne wdrożenia.

KG: Jaką radę dałabyś osobom, które chciałyby pójść podobną ścieżką kariery?

AF: Ujęłabym to w ten sposób „Bądźcie ciekawi i otwarci, nie bójcie się zadawać pytań i popełniać błędów". Cyberbezpieczeństwo to nieustanny proces, który wymaga ciągłego uczenia się, bo krajobraz zagrożeń nigdy nie stoi w miejscu. Rozpoczynając pracę w tej dziedzinie, nie trzeba od razu być ekspertem we wszystkich obszarach. Kluczowe jest znalezienie własnej specjalizacji oraz zachowanie otwartości na współpracę interdyscyplinarną. Równie istotna jest cierpliwość w procesie nauki - rozwój warto traktować jako stopniowy proces, oparty na systematycznym poszerzaniu kompetencji.

Warto też budować sieci kontaktów międzynarodowych i brać udział w projektach - uczą, jak współpracować ponad różnicami i myśleć globalnie. I na koniec - nie bójcie się być sobą. To, że inni myślą inaczej, tylko wzbogaca tę dziedzinę. Znalezienie swojej niszy w cyberbezpieczeństwie to proces, ale warto myśleć szeroko i pracować z różnymi ludźmi - to daje najlepsze efekty. Różnorodność perspektyw jest siłą tej dziedziny, a cierpliwe rozwijanie swoich kompetencji krok po kroku to droga do sukcesu.

KG: Dziękuję za wyczerpujące odpowiedzi. Życzę nowych wyzwań i oczywiście sukcesów na polu naukowym w rozwoju cyberbezpieczeństwa na skalę międzynarodową.

AF: Dziękuję!