Katarzyna Grabowska
NASK

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

Agnieszka Konieczny
Urząd M.St. Warszawy

Rozmowa z Agnieszką Konieczny, Naczelniczką wydziału w Biurze Informatyki Urzędu M.St. Warszawy.

KG: Jakie znaczenie ma dla Ciebie cyberbezpieczeństwo w działalności jednostek samorządu terytorialnego?

AK: W jednostkach samorządu terytorialnego cyberbezpieczeństwo jest dziś priorytetem. Zwiększenie poziomu cyberbezpieczeństwa jest celem wpisanym w strategię rozwoju wielu gmin w Polsce. Mówimy o nim zazwyczaj w kontekście obrony i reakcji na zagrożenia, ale może być też postrzegane jako katalizator transformacji cyfrowej. Cyberbezpieczeństwo to nie „problem IT", nie kwestia technologii i wydatków, to też czynnik wzrostu i rozwoju. W przypadku sektora prywatnego powiedziałabym, że cybersecurity buduje bezpieczeństwo i przewagę konkurencyjną firmy, w sektorze publicznym stanowi tarczę ochronną, która buduje zaufanie mieszkańców do usług publicznych i wpływa na ich rozwój.

KG: Jak postrzegasz rolę kobiet w zarządzaniu projektami z obszaru cyberbezpieczeństwa?

AK: Moim zdaniem rola w zarządzaniu projektami nie powinna zależeć od tego czy jesteś kobietą czy mężczyzną. Od project managera oczekuje się, że zbuduje zaangażowanie w zespole, „dowiezie" w terminie i zgodnie z zakresem, porozumie się z interesariuszami. Te umiejętności są uniwersalne. Płeć nie definiuje kompetencji. Skłamałabym jednak mówiąc, że nie spotkałam się w pracy ze stereotypowym myśleniem czy działaniem. Wciąż funkcjonuje przekonanie, że IT to „męska" dziedzina i czasami muszę

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

udowodnić swoje kompetencje. Bywa, że na spotkaniach pytania są kierowane do kolegów, bo są „techniczni". Raz ktoś spytał – czekamy na PM? Bo rozmówca założył, że PMem jest mężczyzna.

To się zmienia, w IT pracuje coraz więcej kobiet i świetnie sobie radzą. Są wykształcone, zdeterminowane i kreatywne. Nie mają powodów do kompleksów. Zespoły projektowe, które świadomie budują różnorodność zyskują przewagę operacyjną, bo złożone projekty, jak te w obszarze cyberbezpieczeństwa, wymagają spojrzenia z wielu perspektyw.

KG: Jakie przedsięwzięcia związane z cyberbezpieczeństwem były dla Ciebie kluczowe?

AK: Z mojej perspektywy, kluczowe są trzy działania, które stanowią jednocześnie filary bezpieczeństwa organizacji.

Budowa nowej architektury bezpieczeństwa w modelu Cybersecurity Mesh Architecture (CSMA), który umożliwia elastyczną i skalowalną kontrolę bezpieczeństwa wszystkich środowisk (lokalnych, chmurowych, hybrydowych) i danych.

Wdrożenie kompleksowego zarządzania ryzykiem, pozwalającego minimalizować zagrożenia a jednocześnie utrzymywać równowagę między kosztami zabezpieczeń i poziomem akceptowalnego ryzyka.

Budowanie świadomości cyberbezpieczeństwa wśród pracowników i zaangażowanie w projekt osób zajmujących wysokie stanowiska kierownicze w organizacji.

KG: Z jakimi największymi wyzwaniami spotkałaś się podczas zarządzania projektami z obszaru cyberbezpieczeństwa?

AK: Projekty z obszaru cyberbezpieczeństwa

mają swoją specyfikę, która wynika przede wszystkim z ich złożoności.

To nie są tylko projekty informatyczne, których celem jest hardening środowiska, kontrola użytkowników czy detekcja zdarzeń bezpieczeństwa. To nie są też projekty, których celem jest opracowanie dokumentacji normatywnej, tworzącej SZBI czy system zarządzania ciągłością działania. Projekt z obszaru cyberbezpieczeństwa realizowany jest na kilku płaszczyznach jednocześnie – technologicznej, GRC (zarządzanie – ryzyko – zgodność) oraz change management'u (zarządzanie zmianą).

I ta ostania płaszczyzna – zarządzanie zmianą w obszarze cyberbezpieczeństwa – jest zawsze największym wyzwaniem.

Z jednej strony trzeba zarządzać oczekiwaniami interesariuszy, przekonać ich do wdrożenia nowych, skomplikowanych rozwiązań IT i mierzyć się z luką kompetencyjną w zespole projektowym. Z drugiej strony są współpracownicy, którzy muszą wiedzieć, że zagrożenie w sieci jest realne, i że cyberbezpieczeństwo to nie wymysł a konieczność.

Doprowadzenie do sytuacji, w której organizacja wykaże zrozumienie i akceptację dla wdrażanych zmian to zawsze sukces. Dlatego tak istotne w projekcie są komunikacja i edukacja.

KG: Jak nowe technologie mogą stać się elementem strategii cyberbezpieczeństwa miast?

AK: Nowoczesne technologie mogą znacząco zmienić i rozwinąć strategię cyberbezpieczeństwa miast, wymaga to jednak zmiany filozofii działania.

Należy odejść od metody „budowania muru" i stworzyć swego rodzaju układ odpornościowy, który działa jak tarcza - rozpoznaje i niszczy obce elementy oraz własne nieprawidłowe działanie.
Dla wzmocnienia obrony cyberbezpieczeństwa można użyć AI i analityki behawioralnej, których rolą jest zapobieganie incydentom bezpieczeństwa. Wykorzystując rozwiązanie typu SOAR (Security Orchestration, Automation and Response) można zmienić sposób zarządzania cyberbezpieczeństwem np. proces reagowania na incydenty, których obsługa dzięki zastosowaniu SOAR zostanie zautomatyzowana.
Jednak największe znaczenie przypisałabym Bliźniakom Cyfrowym (Digital Twins). Stworzenie wirtualnej kopii infrastruktury IT i odwzorowanie jej działania pozwala wykorzystać Cyfrowego Bliźniaka do symulowania ataków, testowania zabezpieczeń i modelowania skutków incydentów. I wszystko to bez ryzyka dla systemów i usług działających w realu.

KG: Jak widzisz przyszłość roli samorządów w kontekście cyberbezpieczeństwa kraju?

AK: Rola samorządu terytorialnego w kontekście cyberbezpieczeństwa kraju jest kluczowa w dwóch obszarach: zarządzania incydentami bezpieczeństwa i budowania odporności cyfrowej. W sytuacji zagrożeń cyfrowych, samorząd musi zapewnić bezpieczeństwo mieszkańcom i ciągłość działania usług publicznych. Tu ważna jest współpraca, aby w sytuacji takiej, jaka miała miejsce w nocy z 9/10 września 2025 r., kiedy rosyjskie drony naruszyły polską przestrzeń powietrzną,

działania rządu i samorządu były spójne i następowała szybka reakcja. Dlatego samorządy muszą tworzyć nowoczesne strategie cyberbezpieczeństwa i konsekwentnie je realizować, a to oznacza inwestycje w technologie i kompetencje pracowników.

Rząd powinien traktować samorządy jak strategicznego partnera w cyberbezpieczeństwie, ponieważ jest najbliżej mieszkańców, jest wiarygodnym źródłem informacji i buduje zaufanie do działania rządu. Należy odejść od myślenia, że samorząd to administracja. W dzisiejszych realiach silny i świadomy samorząd to element obrony kraju.

KG: Jaką najważniejszą lekcję chciałabyś przekazać tym, którzy chcą podążać podobną drogą zawodową?

AK: Jeżeli mam przekazać jedną radę kobietom, które chcą budować karierę w branży cyberbezpieczeństwa, to jest następująca: nie dajcie się zamknąć w schematy społeczne i wmówić sobie, że to nie dla was. W cyberbezpieczeństwie liczy się umiejętność łączenia kropek – technologii, biznesu i ludzi. To jest zadanie wprost stworzone dla nas.

Lekcja dla wszystkich? Cyberbezpieczeństwo nie lubi ludzi z przypadku – wymaga wiedzy, zaangażowania i ciągłego budowania kompetencji. Nie oznacza to jednak, że musisz znać odpowiedź na każde pytanie. Będąc managerem projektu musisz rozumieć technologię, ale twoja rola to koordynowanie pracy zespołu, komunikacja i zarządzanie ryzykiem. Szczegóły technologiczne zostaw ekspertom.

KG: Dziękuję za rozmowę.

Cyberbezpieczeństwo jest naszą wspólną sprawą i powinniśmy o nie dbać na każdym szczeblu.

AK: Dziękuję!