



Katarzyna Grabowska
NASK



CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

Anna Kwaśnik

Ekspertka ds. budowania
świadomości cyberbezpieczeństwa
w NASK.



*Rozmowa z Anną Kwaśnik, ekspertka ds.
budowania świadomości
cyberbezpieczeństwa w NASK.*

**KG: Jak zmienia się dziś
podejście organizacji do szkoleń
z cyberbezpieczeństwa w kontekście
rozwoju nowych technologii i rosnącej
liczby zagrożeń?**

AK: Podejście organizacji ewoluuje w stronę
dojrzałego zarządzania ryzykiem. Szkolenia
z cyberbezpieczeństwa coraz rzadziej
są postrzegane jako formalny obowiązek,
a coraz częściej jako element strategii
bezpieczeństwa i ciągłości biznesowej. Praca
zdalna, rozwój chmury, narzędzi opartych na
AI czy automatyzacji procesów znacząco
zwiększył odpowiedzialność użytkowników
końcowych.

Z perspektywy menedżerskiej kluczowe staje

się dopasowanie szkoleń do ról, mierzenie ich
skuteczności oraz powiązanie z realnymi
zagroženiami biznesowymi. Organizacje, które
odnoszą sukces, inwestują w proces ciągłej
edukacji, a nie jednorazowe inicjatywy.

**KG: Jakie są dziś największe wyzwania
w budowaniu świadomości
cyberbezpieczeństwa w organizacjach?**

AK: Największym wyzwaniem jest zmiana
postaw, a nie przekazanie wiedzy. Pracownicy
często wiedzą, co „powinni” zrobić, ale
w praktyce działają pod presją czasu, rutyny
i celów biznesowych. Świadomość
cyberbezpieczeństwa przegrywa wtedy
z wygodą, pośpiechem lub innymi zadaniami.
Z perspektywy zarządczej trudnością jest
również utrzymanie ciągłości komunikacji
i zaangażowania. Jednorazowe kampanie
informacyjne nie budują trwałych nawyków.





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

Skuteczna świadomość wymaga systematyczności, spójnych komunikatów oraz wsparcia kadry kierowniczej, która swoim przykładem pokazuje, że bezpieczeństwo jest realnym priorytetem, a nie tylko hasłem. Odpowiedzią na te wyzwania są programy budowania świadomości cyberbezpieczeństwa, które mają charakter kompleksowy i ciągły. Łączą one edukację, komunikację, praktyczne ćwiczenia oraz elementy mierzenia efektów, co pozwala stopniowo utrwalać dobre praktyki i realnie podnosić poziom cyberodporności organizacji. Dzięki temu cyberbezpieczeństwo przestaje być jednorazową inicjatywą, a staje się stałym elementem kultury organizacyjnej.

KG: Wiele programów i kampanii

podnoszących świadomość cyberbezpieczeństwa nie przynosi oczekiwanych efektów – co, według Ciebie, ma na to kluczowy wpływ?

AK: Częstym błędem jest projektowanie kampanii w oderwaniu od realiów pracy organizacji.

Materiały są zbyt ogólne, oderwane od kontekstu lub kierowane do wszystkich w ten sam sposób.

Tymczasem inne zagrożenia dotyczą kadry zarządzającej, inne pracowników operacyjnych, a jeszcze inne zespołów IT.

Dodatkowo kampanie często nie są osadzone w procesach biznesowych i nie mają jasno określonych celów oraz mierników. Bez tego trudno ocenić ich skuteczność i wprowadzać realne zmiany. Świadomość cyberbezpieczeństwa pracowników musi być traktowana jak proces zarządczy, a nie wyłącznie akcja edukacyjna.





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

KG: Jaką rolę pełni kadra menedżerska w budowaniu kultury cyberbezpieczeństwa?

AK: Rola menedżerów jest kluczowa, ponieważ to oni wyznaczają standardy zachowań w organizacji. Jeśli kadra zarządzająca traktuje cyberbezpieczeństwo poważnie, stosuje się do zasad i aktywnie uczestniczy w szkoleniach, pracownicy odbierają jasny sygnał, że bezpieczeństwo jest elementem odpowiedzialności zawodowej.

Z perspektywy zarządzania istotne jest również tworzenie przestrzeni, w której pracownicy mogą zgłaszać incydenty lub wątpliwości bez obawy o konsekwencje.

Kultura cyberbezpieczeństwa opiera się na zaufaniu, transparentności i wspólnej odpowiedzialności, a nie na strachu i karach.

KG: Jakie kompetencje są dziś kluczowe

w zarządzaniu cyberbezpieczeństwem poza wiedzą techniczną?

AK: Zarządzanie cyberbezpieczeństwem w coraz większym stopniu opiera się na kompetencjach miękkich i strategicznych. Kluczowe stają się umiejętność komunikacji, rozumienie procesów biznesowych oraz zdolność przekładania ryzyk technicznych na język zarządczy.

Istotne jest również myślenie systemowe – łączenie technologii, ludzi i procesów w spójną strategię. Cyberbezpieczeństwo przestaje być wyłącznie domeną działów IT, a staje się obszarem wymagającym współpracy wielu interesariuszy na poziomie całej organizacji.

KG: Jaką rolę odgrywają dziś kobiety w obszarze cyberbezpieczeństwa i jakie kompetencje są szczególnie istotne z perspektywy organizacji?





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

AK: Kobiety coraz częściej odgrywają kluczową rolę w cyberbezpieczeństwie, zwłaszcza w obszarach wymagających łączenia technologii z zarządzaniem, komunikacją i edukacją. Organizacje potrzebują dziś nie tylko specjalistów technicznych, ale także liderów, którzy potrafią budować świadomość, zarządzać ryzykiem oraz skutecznie współpracować z biznesem – i to są kompetencje, w których wiele kobiet naturalnie się odnajduje. Szczególnie istotne są umiejętności analitycznego myślenia, rozumienia zachowań użytkowników, prowadzenia dialogu z kadrą zarządzającą oraz projektowania programów edukacyjnych dopasowanych do różnych grup odbiorców. Kobiety często wnoszą także perspektywę długofalową – skupioną na procesach,

kulturze organizacyjnej i trwałej zmianie nawyków, a nie wyłącznie na reagowaniu na incydenty. Z perspektywy zarządczej różnorodność zespołów cyberbezpieczeństwa zwiększa ich skuteczność. Łączenie kompetencji technicznych z kompetencjami społecznymi i menedżerskimi pozwala organizacjom lepiej odpowiadać na dynamicznie zmieniające się zagrożenia i budować realną odporność cyfrową.

KG: Dziękuję za rozmowę dotyczącą bardzo ważnego tematu jakim jest budowanie świadomości cyberbezpieczeństwa ☺

AK: Dziękuję!

EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA

