aut. Szymon Palczewski 07.01.2019

NOWY RAPORT O STANIE CYBERBEZPIECZEŃSTWA UE. ENISA SKUPIONA NA OBYWATELACH

ENISA opracowała nowy raport na temat stanu cyberbezpieczeństwa UE. „Analysis of the European R&D. Priorities in cybersecurity", który prezentuje kluczowe dziedziny bezpośrednio związane z zagrożeniami cyfrowego świata. W dokumencie podkreślono znaczenie obywateli oraz unijnych regulacji w zakresie kształtowania kompleksowego bezpieczeństwa Wspólnoty.

Głównym celem dokumentu jest identyfikacja zagrożeń dla społeczeństwa europejskiego w zakresie cyberbezpieczeństwa oraz określenie priorytetów badań, które mają przyczynić się do zwalczania incydentów, zanim te się zmaterializują. Identyfikując przyszłe obszary problemowe, Unia Europejska może podjąć proaktywne działania na rzecz obrony przed przewidywanymi zagrożeniami. Kluczowe w tym zakresie jest bezpieczeństwo informacji ze względu na nieustającą cyfrową transformację.

W oparciu o badania i współpracę z ekspertami, ENISA zidentyfikowała kluczowe procesy oraz zmiany w społeczeństwie europejskim spowodowane innowacjami w cyfrowo połączonym świecie. Specjaliści zwrócili uwagę na współzależność świata wirtualnego i fizycznego, wszechobecność łączności, a także ewolucję technologii oraz ich wpływ na społeczeństwo.

Raport koncentruje się na identyfikacji wyzwań, które są istotne z punktu widzenia obywateli państw członkowskich UE. Nowoczesna technologia potęguje wpływ pojawiających się zagrożeń na życie jednostek. W tym zakresie nabiera znaczenia edukacja oraz podnoszenie świadomości społeczeństwa w odniesieniu do analizy zagrożeń lub ryzyka.

Dokument identyfikuje obszary, które wymagają większej uwagi w zakresie cyberbezpieczeństwa:

1. Budowanie świadomości (obszar społeczny):
   - uwzględnienie w społeczeństwie potrzeby uświadamiania wpływu zmian technologicznych na ewolucję społeczną, a tym samym na ryzyko społeczne;
2. Budowanie zdolności (obszar edukacji):
   - brak specjalistów ds. cyberbezpieczeństwa, w związku z tym konieczność wdrożenia środków podnoszenia wiedzy na poziomie średnim i wyższym w celu uzupełnienia deficytów;
3. Zagrożenia egzystencjalne (obszar zagrożeń mogących zniszczyć całe społeczeństwo, przemysł lub biznes):
   - sztuczna inteligencja (AI) – dzięki zbieraniu danych, mocy obliczeniowej i pojemności pamięci sztuczna inteligencja będzie rozwijać się z wielką szybkością, niosąc nowe możliwości, ale i ryzyko;
   - technologie kwantowe – mogą być stosowane zarówno w atakach przeciwko obecnym metodom ochrony kryptograficznej, jak i w opracowywaniu nowych modeli obliczeniowych w celu dalszego rozwoju oraz przyspieszenia zmian;
   - cyberprzestępczość – dzięki cyfrowej transformacji, wirtualnej tożsamości oraz cennym zasobom każdy może stać się ofiarą podczas cyberataku. Wykrywanie i łagodzenie incydentów

staje się niezwykle istotne;
- zagrożenie prywatności – wzrasta wraz ze zbiorami danych, które mogą zostać naruszone i wykradzione.

Budowanie świadomości - wyzwanie społeczne

W raporcie ENISA podkreśla, że cyfrowa transformacja jest przykładem zmiany społecznej, która wpływa na zachowanie jednostek. Tempo owej transformacji sprawia, iż wiele obywateli nie jest świadomych pojawiających się nowych zagrożeń. Do tej pory prowadzone kampanie na rzecz cyberbezpieczeństwa nie przynosiły pożądanych rezultatów.

W związku z tym cyberbezpieczeństwo musi stać się wspólną odpowiedzialnością, a wszystkie podmioty zaangażowane powinny działać na rzecz poprawy bezpieczeństwa cyfrowego świata. W tym celu konieczne jest zrozumienie powiązanych zagrożeń, a także sposobów ich zabezpieczenia i ochrony przed nimi. Taki stan rzeczy wymaga z kolei zrozumienia ludzkich zachowań oraz psychologii zmian, w tym zasad funkcjonowania społeczeństw. Połączenie wielu dyscyplin nauki jest jedną z dróg, dzięki którym można bezpiecznie zarządzaćtransformacjami, wynikającymi ze zwiększonej cyfryzacji społeczeństwa.

W tym zakresie ENISA zaleca podjęcie działań mających na celu zaprojektowanie odpowiednich narzędzi oraz środków bezpieczeństwa, które będą przyjazne dla społeczeństwa (np. intuicyjne interfejsy). Równie istotne jest rozwijanie innowacji w zakresie informowania o cyberzagrożeniach, a także lepsze rozumienie obywateli, w jaki sposób korzystają z technologii.

Budowanie potencjału - wyzwanie edukacyjne

W raporcie użyto stwierdzenia, że „budowanie cyberbezpieczeństwa nie powinno być podejmowane wyłącznie z technologicznego punktu widzenia, ponieważ posiada holistyczną perspektywę". Eksperci ds. bezpieczeństwa cybernetycznego powinni skupiać się nie tylko na technologii, ale również na aspektach organizacyjnych, a także zachowaniach ludzi zarówno na poziomie indywidualnym, jak i społecznym.

Bezpieczeństwo jest złożonym zagadnieniem, które musi być brane pod uwagę w każdym elemencie podczas całego cyklu życia produktu lub usługi. Należy również podchodzić do niego z punktu widzenia systemu, ponieważ tylko w ten sposób można dostrzec współzależność komponentów i ich zintegrowanie z całością.

W dokumencie podkreślono, że poszerzenie tematyki na kursach informatycznych stworzy nową generację profesjonalistów, którzy będą rozumieć podstawy bezpieczeństwa oraz posiadać umiejętności tworzenia oprogramowania z myślą o prywatności i bezpieczeństwa w w sensie kompleksowym.

Sztuczna inteligencja - szansa i zagrożenie

Sztuczna inteligencja w swej istocie jest ogromną korzyścią i szansą. Jednak jej powstanie oraz rozwój wiąże się również z dużym ryzykiem. Dzięki zbieranym danym, szybką łącznością oraz infrastrukturą chmury, każdego dnia promowane są nowe aplikacje korzystające z rozwiązań w zakresie sztucznej inteligencji. Współcześnie atrakcyjność wdrażania AI do przedsiębiorstw jest znaczna, a jej zasięg nieustannie się powiększa.

W tym zakresie ENISA proponuje skupienie się na promocji bezpiecznej i integralnej sztucznej inteligencji, której ludzie będą mogli zaufać. Niemniej istotna jest również weryfikacja, bezpieczeństwo oraz regularna kontrola algorytmów uczenia maszynowego tak, aby dane wejściowe nie zostały

zmanipulowane.

Technologia kwantowa

W raporcie stwierdzono, że w wielu projektach badawczych związanych z technologią kwantową istnieje wiele kluczowych wyzwań oraz problemów rozwojowych, a uzyskanie wyników może wymagać wielu lat.

Wśród zaleceń dla tego obszaru wskazano na konieczność podjęcia działań mających na celu ułatwienie prowadzonych badań nad kryptografią kwantową oraz innymi podobnymi rozwiązaniami. Kluczowe jest także wspieranie rozwoju sieci szybkich geograficznych dystrybucji danych kwantowych (np. za pomocą łączy satelitarnych oraz naziemnych) dla zapewnienia komunikacji o wysokim poziomie bezpieczeństwa.

Zagrożenia łańcucha dostaw

Coraz więcej sektorów gospodarki jest zależnych od infrastruktury cyfrowej. W związku z tym utrata integralności lub naruszenie poufności może mieć poważne konsekwencje nie tylko dla przedsiębiorstw, ale także rządów, które korzystają z ich usług. Idąc dalej, niedostępność operacji finansowych, będąca skutkiem cyberataku, może negatywnie wpłynąć na gospodarkę większości państw, w tym samych przedsiębiorstw.

ENISA zdaje sobie sprawę, że bezpieczeństwo systemów nie może być w pełni zagwarantowane. Niemniej jednak w dokumencie stwierdzono, iż należy dołożyć wszelkich starań, aby chronić systemy w celu redukcji ryzyka do akceptowalnego poziomu oraz zapewnić odporność, a także ciągłość działania procesów.

Cyberprzestępczość – wykrywanie, zwalczanie i atrybucja

W raporcie zauważono, że działalność przestępcza w sieci nieustannie się rozwija. Dzięki cyfrowej transformacji wiele cennych zasobów jest dostępnych online, co może zostać wykorzystane przez cyberprzestępców. Hakerzy dla swoich celów wykorzystują powszechnie znane i sprawdzone metody, jednak ich działalność ewoluuje. Opracowują oni nowe, bardziej wyrafinowane rozwiązania oraz techniki działania.

ENISA zaleca w tym zakresie prowadzenie badań odnoszących się do priorytetów technicznych dotyczących wysiłków na rzecz podnoszenia cyberbezpieczeństwa oraz opracowywania innowacyjnych narzędzi w celu zwiększenia świadomości sytuacyjnej.

Wyzwania dla prywatności

W dokumencie odwołano się do zapisów Powszechnej Deklaracji Praw Człowieka oraz Karty Praw Podstawowych, gdzie prywatność uznano za podstawowe prawo przynależne człowiekowi. W związku z tym podkreślono znaczenie rozporządzenia o ochronie danych osobowych (RODO), które nakłada na podmioty obowiązek wdrożenia odpowiednich środków na rzecz ochrony i bezpieczeństwa procesów przetwarzania danych. Według raportu tego typu rozwiązanie pomaga chronić prywatność obywateli.

W związku z tym ENISA rekomenduje promowanie i rozpowszechnianie technologii zwiększających prywatność w różnych komponentach (np. chmurze danych czy IoT) oraz za pomocą aplikacji. Nie mniej istotny jest rozwój oraz doskonalenie narzędzi oceny prywatności, ponieważ tylko w ten sposób można uzyskać rzetelne wyniki w odniesieniu do poziomu ochrony danych obywateli.