Cyberbezpieczeństwo w erze AI i IoT. Działania Samsung na rzecz ochrony użytkowników

Tomasz Chomicki
Dyrektor ds. rozwoju biznesu, Samsung Electronics Polska

W Samsung zdajemy sobie sprawę ze znaczenia bezpieczeństwa i prywatności naszych użytkowników. Rozwiązania elektroniki konsumenckiej takie jak rozwiązania mobilne, tj. telefon, tablet, ale też lodówka czy odkurzacz są narażone na coraz większą liczbę zagrożeń wynikających z szybkiego rozwoju i ewolucji technologii za pośrednictwem platform mobilnych, Internetu rzeczy (IoT), urządzeń i infrastruktury sieci 5G.

W lutym b.r. jedna ze spółek grupy Samsung – Samsung SDS opublikowała ważny raport dotyczący zagrożeń.

Firma przeanalizowała problemy związane z cyberbezpieczeństwem, które wystąpiły w Korei i poza nią w zeszłym roku i przedstawiła kilkakluczowych zagrożeń związanych z cyberbezpieczeństwem.

Są one następujące:

- konieczność przygotowania się na phishing oparty o algorytmy sztucznej inteligencji (AI);
- „zagrożenia bezpieczeństwa chmury" z powodu braku dbałości o dane uwierzytelniające użytkowników; - „ataki ransomware" ewoluujące w podwójną strategię wymuszenia;
- „zagrożenia bezpieczeństwa łańcucha dostaw oprogramowania" z powodu infiltracji złośliwego oprogramowania typu open source;
- zagrożenia bezpieczeństwa infiltrujące OT i IoT – podatności w hiperpołączonym społeczeństwie.

Opracowanie powstało w oparciu o wywiady z około 400 ekspertami ds. bezpieczeństwa z z branży produkcyjnej, finansowej i logistycznej oraz z sektora publicznego czy obronnego. Raport pokazuje nie tylko co jest zagrożeniem, ale daje też cenne wskazówki jakie działania należy podjąć.

Z raportu Microsoft Digital Defense Report opublikowanego w październiku 2025 r. wynika, że Polska znalazła się w czołówce najbardziej atakowanych państw Europy. Rosnąca skala ataków stała się dziś nową rzeczywistością. Cyberbezpieczeństwo to nie tylko wyzwanie i problem technologiczny, przed którym postawione są zespoły techniczne, ale zadania, z którymi zmierzyć musi się każdy z nas. Samsung w Polsce podejmuje szereg zakrojonych działań, które służą budowie cyberoodporności.. Są to m.in. porozumienia o działań w ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber) wpisują się one w politykę edukowania o cyberbezpieczeństwie nowoczesnych technologii. PWCyber został uruchomiony w 2019 r. Jest to przedsięwzięcie niekomercyjne o charakterze partnerstwa publiczno-prywatnego, realizowane na rzecz krajowego systemu cyberbezpieczeństwa. Innym przykładem działań jest podpisana w 2024 r. umowa z Dowództwem Komponetu Wojsk Obrony Cyberprzestrzeni.

Od lat zespoły projektowe Samsung bardzo poważnie traktują aspekty cyberbezpieczeństwa i prywatność produktów tworząc gamę nowoczesnych rozwiązań. Nieomal we wszystkich jednostkach biznesowych firmy Samsung działają dedykowane zespoły ds. bezpieczeństwa, które stale przeprowadzają audyty produktów i usług firmy. To działanie ma zapewnić stałą ochronę bezpieczeństwa i prywatności naszych użytkowników oraz pracowników organizacji.

Jednym z wyzwań, ale również naszych priorytetów jest jak najszybsze reagowanie na pojawiające się zagrożenia i luki w zabezpieczeniach. Należy pamiętać, że niektóre jednostki biznesowe firmy Samsung oferują program nagród za zgłoszone luki w zabezpieczeniach.

W firmie Samsung posiadamy innowacyjną inicjatywę w której bardzo cenimy społeczność „badaczy" cyberbezpieczeństwa. Ich praca służy jak najszybszemu usuwaniu potencjalnych luk w zabezpieczeniach. Ich ujawnianie pomaga zapewnić bezpieczeństwo i prywatność klientów końcowych.

Poprzez te działania:

- dokładamy wszelkich starań, aby uniknąć naruszeń prywatności, pogorszenia jakości obsługi użytkownika, zakłóceń w działaniu serwerów wewnętrznych lub zewnętrznych oraz zniszczenia danych lub zasobów fizycznych podczas testów bezpieczeństwa;
- stosujemy się do wytycznych dotyczących raportowania, aby jak najdokładniej przedstawić szczegóły potencjalnych luk w zabezpieczeniach;

W zamian zobowiązujemy się do:

- współpracy, aby szybko zrozumieć i rozwiązać potencjalną lukę w zabezpieczeniach;
- dołożenia wszelkich starań, aby usunąć luki w zabezpieczeniach i udostępnić poprawki użytkownikom końcowym w ciągu 90 dni;

Źródło : https://security.samsungmobile.com/
https://www.samsungsds.com/en/news/cybersecurity-250220.html
https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/