26.07.2024 r.

#341

TRANSKRYPT ODCINKA

Apple i nasze bezpieczeństwo (Mariusz Pik)

Partnerem tego podcastu jest iMAD.pl – współpraca płatna.

[MUZYKA]

Tu Krzysztof Kołacz, a ty słuchasz właśnie podcastu, „Bo czemu nie?”. Usłyszysz w nim o technologiach, które nas otaczają i nas w tych technologiach zanurzonych. Sprawdzam, pytam i podpowiadam jak korzystać z nich tak, aby to one służyły nam, a nie my im.

W dzisiejszym odcinku o bezpieczeństwie, czyli dlaczego Apple jest uznawane i faktycznie jest najbezpieczniejszym dostawcą usług i urządzeń na świecie? Pogadałem o tym z moim gościem – Mariuszem Pikiem, ekspertem iMAD do spraw wdrożeń MDM.

Proszę, zostaw opinię na Apple Podcasts lub na Spotify. Twój głos ma znaczenie!

Zaczynamy.

[MUZYKA CICHNIE]

[KRZYSZTOF] Dzisiejszy odcinek poświęcamy, właściwie wspólnie z moim gościem, którego zaraz Wam będę miał zaszczyt przedstawić, tematowi, który jest szalenie istotny z punktu widzenia nie tylko dyskusji w naszym apple’owskim środowisku w Polsce, ale również z punktu widzenia takiego zwykłego użytkownika. Tego, który idzie sobie do salonu kupić sobie nowy sprzęt od Apple, jakikolwiek sprzęt i gdzieś z tyłu głowy zawsze ma to hasło: „Apple jest bezpieczne! Apple to jest prywatność”. No i właśnie, okazuje się, że kiedy pójdziemy głębiej w tych dyskusjach, kiedy na przykład Wy też piszecie w formularzu kontaktowym do mnie, czy na kontakt@boczemunie.pl, gdy pojawia się ten wątek w Waszych wiadomościach o prywatności, to zawsze kończy się mniej więcej tak samo, czyli ja wysyłam jakieś dokumenty, źródła na stronach Apple dostępne oficjalnie języku polskim i się

okazuje, że nikt nie wie o ich istnieniu… O nich również dzisiaj powiemy. Powiemy, gdzie szukać tych informacji na temat tego, jak Apple jest bezpieczne, dlaczego jest bezpieczne, w jaki sposób przetwarza dane użytkowników, nasze dane i dlaczego warto właśnie tej firmie zaufać, jeżeli szukamy kogoś, kto dostarczy nam i zapewni platformę *software*'*ową* i *hardware*'*ową* bezpieczną właśnie.

A moim i Waszym gościem, który mi w tym dzisiaj pomoże i też opowie o swojej drodze z tą firmą, jak to w tym podcaście bywa od lat, jest Mariusz Pik, ekspert iMAD do spraw wdrożeń MDM w korporacjach, szkołach i nie tylko.

Cześć Mariusz!

[MARIUSZ] Cześć, dzień dobry, witaj.

[KRZYSZTOF] Mariusz, bardzo się cieszę, że dołączyłeś do tego odcinka i na początek będę Cię prosił standardowo, jak każdego mojego gościa, który jest w jakiś sposób fanem Apple, mniejszym lub większym, aby opowiedział nam o tym, jak się ta przygoda w ogóle zaczęła? Od kiedy Ty jesteś z firmą Cupertino związany prywatnie, jako użytkownik oczywiście?

[MARIUSZ] Tak naprawdę moja fascynacja Apple zaczęła się jeszcze podczas studiów. Natomiast pamiętasz tego białego MacBooka, który kiedyś, kiedyś lata temu był dostępny u nas. To był mój pierwszy MacBook kupiony jeszcze w jednej z sieci dużych elektro marketów u nas w Polsce.

[KRZYSZTOF] To ta mydelniczka taka, co miała ten topkę i co pękał!

[MARIUSZ] Tak, udało mi się tego uniknąć, chociaż muszę przyznać, że ta mydelniczka, jak ty ją nazwałeś, była wyjątkowo podatna na wszelkiego rodzaju rysy i zabrudzenia. Niemniej jednak dostarczała niesamowitej przygody i fanów z użytkowania.

[KRZYSZTOF] To był chyba taki sprzęt, który tak jak patrzyłeś, to kojarzył się jak białe słuchawki do dziś. W sensie to było – Apple!

[MARIUSZ] Tak, bo to było takie piękne, takie fajne, takie zupełnie inne niż to, co można było zobaczyć na półkach. No i to doświadczenie samego użytkowania tego

sprzętu było niesamowite, chociaż, przyznam szczerze, nie wiedziałem wtedy wiele o bezpieczeństwie sprzętu.

[KRZYSZTOF] Tak, no w ogóle wtedy jak się miało Apple, jak się przychodziło do, nie wiem, na kampus uniwersytecki, to było się królem, albo jak się w ogóle pojawiałeś z nim na mieście, gdzieś to jeszcze były początki tych słynnych trendów, pójdę z Makiem do kawiarni, wiadomo jakiej i sobie siądę i będzie jabłuszko świecić, no to był, byłeś kimś, nie. W sensie to był totalny szpan i lans, nie?

[MARIUSZ] Nikt nie dyskutował o produktywności czy bezpieczeństwie, ale za to można było pozostać zostać wskazywanym palcem w miejscu publicznym.

[KRZYSZTOF] Tak, oczywiście, że tak. Natomiast ja tam z nostalgią patrzę w kierunku tamtej i chciałbym kiedyś zobaczyć taki powrót do retro korzeni trochę. Jakieś malowanie, czy to perłowe, czy jakkolwiek by to dziwnie teraz Apple nazywało. Wtedy nikt nie nazywał w ten sposób sprzętów jak dzisiaj, bo to by było fajny ukłon w kierunku tych, którzy pamiętają te tamte czasy.

[MARIUSZ] Wiesz, że chodzą takie słuchy a propos nowych premier, Apple Watchy na przykład w wersji SE…

[KRZYSZTOF] No słyszałem. Zresztą mieliśmy już Apple Watcha perłowego, nie? W sensie on był ceramiczny.

[MARIUSZ] Tak. Bardzo ładna była ta wersja.

[KRZYSZTOF] Śliczny. Wydaje się, że jeden z najpiękniejszych projektów Jony’ego Ive’a, zdecydowanie piękniejszy niż ten złoty, który kosztował 100 tysięcy złotych i wszyscy wiemy jak skończył… Też, mi się tak wydaje, absolutnie wyróżniał się tutaj. I był bardzo, bardzo taki apple’owski. iPhone’a kiedy pierwszego nabyłeś? Pamiętasz początki iPhone'ów w ogóle nad Wisłą, czy to było później?

[MARIUSZ] Oczywiście, że tak! Te pierwsze iPhone'y, powiedzmy, nie były do końca takie legalne, bo wiadomo, ktoś sobie przywiózł. No i zobaczyłem tego pierwszego iPhone’a i WOW, po prostu WOW, że nagle w takim małym urządzeniu może być ukrytych tyle funkcji. A posługiwałem się wtedy też bardzo dobrym smartfonem jednego z czołowych producentów, nawet z klapką, ale to był, tak, ale to był nadal jednak smartfon, prawda. Miał taki malutki ekranik, miał te klawisze i tak dalej.

Nawet można było sobie pograć w jakieś rzeczy, ale gdy się wzięło do ręki tego iPhone'a, jeden z moich kolegów łaskawie mi go pokazał, no to było po prostu odkrycie, bo nagle zobaczyłem, że naprawdę mam w dłoni taki minikomputer, z którym mogę o wiele, wiele, wiele więcej. No i oczywiście od tego czasu chciałem mieć swój własny, no i był to 3GS. To wtedy zaczęła się moja przygoda z iPhone'em, chociaż oczywiście wcześniej jeszcze miałem iPody, tak?

[KRZYSZTOF] Dużo tego miałeś? Tych iPodów? Bo ja mam do dzisiaj jakąś małą kolekcję tu w domu i jak sobie nieraz naładuję któregoś i tam jest dalej wygrana Nora Jones i jej słynne albumy jakieś, czy tam Beatlesi, to sobie podłączę na przykład, wiesz, do jakichś słuchawek, tak no wejdźmy do AirPods Maxów, których teraz mam, przez kabelek podłączę to dalej uważam, że tamte przetworniki, które były w tych iPodach montowane – pod kątem takiego, nie wiem jak to po polsku powiedzieć, po angielsku powiedziałbym *raw sounds*, w sensie takiego czystego, rdzennego, odartego dźwięku ze wszystkich możliwych udoskonaleń, Spatial Audio i nie wiadomo czego – brzmiały lepiej.

[MARIUSZ] To prawda, tym bardziej, że też zauważyłem wtedy, a wraz z twojego pytania, to chyba, no miałem cztery iPody. Natomiast to był też czas, kiedy producenci audio, ci tacy niszowi, dostrzegali możliwości tego iPoda i tworzyli do niego różnego rodzaju wzmacniacze słuchawkowe. Nawet widziałem wzmacniacze lampowe, które obsługiwały iPodem. To było jednak niesamowite doświadczenie, ale umówmy się, że wtedy proces zakupu muzyki w Polsce tak naprawdę nie istniał.

[KRZYSZTOF] Istniał, to się nazywało CloneCD.

[MARIUSZ] Tak właśnie! A okładkę trzeba było sobie ściągać z internetu.

[KRZYSZTOF] Tak, aczkolwiek ja pamiętam jak moi rodzice podpięli mi pierwszą kartę, chyba Inteligo to wtedy tylko działało z iTunesem i ja zacząłem kupować piosenki. I ty wiesz, że od tamtego momentu, to było tak dawno temu, rany jak dawno… I ja już nic później nie piraciłem. W sensie to po prostu się stało dla mnie tak, kurczę mówiąc zupełnie wprost, tak oczywiste, że nawet, że trzeba było wtedy na album to uskładać kasy jeszcze w tamtych czasach, ale kurczę, było to tak oczywiste, że po prostu przestałem rozumieć sens czegokolwiek innego i to właśnie zrobiło dla całego świata Apple i dla rynku muzycznego przede wszystkim iTunesem, bo to nie jest tylko moja opinia, wiele osób tak miało z tamtego pokoju.

[MARIUSZ] Przeszedłem dokładnie taką samą ścieżkę, mimo tego, że niektórzy znajomi mówią mi, ale po co kupujesz? Wiesz, są inne źródła? Ale tak naprawdę w moim odczuciu, w moim przekonaniu, już pomijając fakt, że to było po prostu legalne, to po prostu – wygoda. Niesamowita wygoda, bo nagle zacząłem korzystać z tej funkcji, którą Apple wprowadziło mimochodem albo nie. Po prostu nie trzeba było kupować całych albumów. Można było sobie wybrać tę piosenkę, którą chciałeś słuchać, którą chciałeś mieć zapodaną każdego poranka, żeby lepiej zaczynać dzień. I to było niesamowite! I w ten sposób mogłeś sobie tworzyć i tworzysz do tej pory playlisty, takie jakie chcesz.

[KRZYSZTOF] Bo tak się zaczęły! To nie streaming zaczął playlisty, to też mało osób o tym jest w ogóle z tego pokolenia, że tak powiem aktualnie wchodzącego gdzieś tam na rynek pracy, to nikt nie jest z tego prawie świadomy, natomiast no tak było, nie, w sensie wiem, że część z moich słuchaczy też do niego przynależy, więc – no moi drodzy, playlisty zaczęły się od kupowania pojedynczych piosenek i układania ich w domu, a jeszcze wcześniej zaczęły się od składanek na płytach CD na Windowsie jeszcze dla pierwszych miłości! Piękne czasy… Ale żeśmy sobie retro początek zrobili, bardzo się cieszę, bo ja lubię w wakacje tak pogadać o takich, jakoś mnie zawsze w wakacje nachodzi, jak jest ten sezon ogórkowy w premierach na jakieś takie retro wspominki, czy właśnie wygrzebywanie z szafy starych urządzeń, no bo jakoś tak więcej czasu wtedy może się człowiek na refleksję pokusić, o refleksję pokusić.

[MARIUSZ] Absolutnie tak!

[KRZYSZTOF] Mariusz, na co dzień zajmujesz się wdrożeniami MDM.

Zaczniemy sobie od tego, bo to gdzieś jest sobie najbliższe. To od razu Ciebie zapytam, bo o to też mnie słuchacze pytają i to się nierozerwalnie wiąże z tematem bezpieczeństwa, bo któż nie szuka bezpieczeństwa jak organizacje, korporacje czy edukacja szeroko rozumiana. Jak to wygląda z punktu widzenia Twojego nad Wisłą? Bo to jest taki trochę temat persona non grata. W sensie on się pojawia i wszyscy w pomieszczeniu milkną. Wiem, że nie możesz o liczbach mówić, ale jaka to jest Mariusz skala? W sensie, czy to jest tak, że przychodzą firmy i mówią, słuchajcie, mamy już dość tego czy innego systemu, chcemy się przenieść na Apple'a, ale kompletnie jak dziecko we mgle nie wiemy od czego zacząć. Czy to jest, wiesz, że przychodzą tylko nerdy. Jak to jest?

[MARIUSZ] Trochę tak. Trochę masz rację. Trochę mówię, dlatego, że myślę, że na to trzeba spojrzeć szerzej. Otóż w Polsce, nie tylko w Polsce, w tej części Europy wiemy, jaki system jest systemem dominującym. W związku z tym informatycy praktycznie wiedzą wszystko na temat obsługi tego właśnie systemu. Apple, nawet jak zobaczysz na wyniki sprzedaży, jest nadal, może nie zajmuje pozycji marginalnej, natomiast nie jest za bardzo rozpowszechniany w Polsce. I to ma oczywiście przełożenie na to, co ja robię. Dlatego, że dla wielu firm taka definicja albo taka fraza zarządzanie sprzętem Apple jest czymś zupełnie zgoła niedocenionym, nieznanym. To jest w ogóle taka, wiesz, terra incognita? Tak to chyba można by nazwać.
Firmy nie mają doświadczenia w tego typu rzeczach. Nie wiedzą, jak zarządzać sprzętem Apple – nie wiedzą, z czym to się je. I tutaj zaczyna się tak naprawdę moja rola, żeby pokazać moim klientom, że zarządzanie sprzętem Apple to przede wszystkim bezpieczeństwo, ale bezpieczeństwo bardzo szeroko rozumiane, bo to jest bezpieczeństwo firmy. Mało tego, na pewno zwróciłeś uwagę, mogłeś zwrócić uwagę, a ja jestem tego świadkiem praktycznie na co dzień. Bardzo dużo firm ma w naszym kraju źle zaprojektowaną ścieżkę wdrożenia sprzętu Apple w firmie. My to nazywamy *onboarding*, prawda?

[KRZYSZTOF] Czy w ogóle sprzętu i pracownika razem w jednym koszyku wzięto, bo to po prostu nad Wisłą leży, o ile to nie jest korporacja ze Skandynawii czy z USA.

[MARIUSZ] Ja bym to sprowadził do prostej ścieżki. Otóż wyobraź sobie, że dana firma nabywa sprzęt Apple. Ten sprzęt Apple ląduje gdzieś tam na biurku administratora IT albo działu odpowiedzialnego za dystrybucję tego sprzętu. Ten sprzęt po numerach seryjnych jest wprowadzany do jakiejś bazy danych, najczęściej jest to Excel, po czym na mocy albo za pomocą jakiegoś tam protokołu odbioru czy protokołu przekazania, ten sprzęt ląduje na biurku użytkownika. I co się dzieje dalej. I ten użytkownik najczęściej loguje się swoimi danymi prywatnymi, bo ma jakieś swoje prywatne konto Apple ID. Wyobrażasz sobie, co w tej chwili się dzieje, który pracuje w danej firmie, loguje się prywatnymi poświadczeniami swoimi na swoim komputerze. I teraz tutaj dotykamy tej niewiedzy, tego braku kompetencji, bo z punktu widzenia administratora ja w tym momencie tracę kontrolę nad tym sprzętem, który jest sprzętem firmowym. Gdyby cokolwiek się stało, na przykład ten komputer wrócił do mnie nadal z poświadczeniami prywatnymi danego użytkownika, to ja nie mógłbym z tym komputerem nic zrobić, no chyba, że zacznę

udowadniać firmie Apple, że ten komputer rzeczywiście był nabyty przeze mnie. No ale to jest procedura raczej czasochłonna.

[KRZYSZTOF] Tak, plus jeszcze jedna kwestia, na pewno nikt prywatnie nie wyłączy też Find My, no to już w jakiś sposób „ucegli", o czym sobie później powiemy ten komputer. I powiem Ci, że ja nie tylko się nie dziwię temu przykremu obrazkowi, który nam tutaj opisałeś, czy przedstawiłeś, ale ja go pamiętam. Pamiętam go jeszcze sprzed wielu lat z jednej dużej marki odzieżowej w Polsce, która niby w ofertach dawała możliwość wyboru komputerów pracownikom, tylko że tych nie Windowsów, czyli Maców używało tam, promil ludzi tam używało ich, nie. I jak zawsze trafił jakiś jegomość, który chciałby mieć Maca, to owszem, on go dostawał, tylko że to… zatrzymując się na tym biurku administratora – to już wtedy wyglądało tak, że on przychodził nawet do tego pokoju administratora i ten administrator mówił mu wprost: Słuchaj, jest dla ciebie Mac, tylko że ja nie mam pojęcia co z nim zrobić, włącz go, żebym mógł spisać numer seryjny. Nawet nie wiedział, że on jest normalnie na urządzeniu nadrukowany i sobie go po prostu weź i sobie go używaj jak sobie chciałeś Maca mieć… No i to jest paranoja, żeby nie powiedzieć patologia.

[MARIUSZ] Powiem Ci więcej. Wyobraź sobie i na pewno też znasz tę sytuację, gdy sprzęt Apple w dużych firmach jest raczej sprzętem, no wiadomo, półki premium, raczej tak jest traktowany, w związku z tym on trafia raczej do kadry kierowniczej, łącznie z prezesami. Nie uwierzysz, a być może wiesz, z iloma stanowiskami tego typu spotkałem się, z iloma prezesami rozmawiałem, którzy twierdzili, że oni absolutnie nie chcą mieć zarządzanego iPhone'a czy zarządzanego MacBooka. Dlaczego? Dlatego, że boją się, że administrator będzie podglądał to, co on robi z tym swoim urządzeniem. Zupełne nieporozumienie w przypadku zarządzania sprzętem Apple. Biorąc pod uwagę, jak Apple podchodzi do ochrony danych osobowych.

[KRZYSZTOF] A jak do nich podchodzi i od tego sobie zaczniemy, zaraz Wam o tym powiemy. Jeszcze tylko jeden *disclaimer* na sam początek tego tematu prywatności.

Wszystko, o czym tutaj opowiadamy, nie zwalnia Was, moi drodzy, z logicznego myślenia!

To jest absolutna podstawa i tak samo jak absolutną podstawą jest to, żeby się oburzyć, kiedy się słucha podcastów technologicznych takich jak ten i jemu

podobne. Gdy np. administrator Wam powie, że on nie wie jak włączyć w firmie Waszego Maca, tak samo uprawnione jest logiczne myślenie w ogóle w codzienności, do czego zawsze zachęcam w tym podcaście, żeby intencjonalnie żyć i świadomie, więc w tym temacie również nie ma żadnych wyjątków.

A zacznę sobie od takiego cytatu, który można znaleźć w dokumentach Apple, do których linki znajdziecie w opisie do tego odcinka pod adresem boczemunie.pl/341/, a który mówi o swego rodzaju fundamencie DNA tematu prywatności, czym jest dla Apple. I brzmi on tak:

> *Prywatność jest podstawowym prawem człowieka i jednym z fundamentów Apple. Dlatego nasze produkty i usługi projektujemy tak, aby jej strzegły. Innowacyjność w tej dziedzinie ma dla nas ogromne znaczenie. Apple szanuje podstawowe prawa do prywatności i uważa, że powinny być takie same na całym świecie. Z tego względu wszystkie dane, które dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (lub firmy w domyśle), lub są z nią powiązane, według Apple uznawane są za „dane osobowe" niezależnie od miejsca zamieszkania tej osoby lub stacjonowania floty firmowej i są objęte ochroną prywatności.*

Mało tego, dla Apple większość z tych danych to są dane totalnie anonimowe, z wyjątkami takimi, które anonimowe oczywiście nie mogą być. Zaraz sobie o tym powiemy więcej, ale to zdanie, że prywatność jest podstawowym prawem człowieka, myślę, że Mariusz jest dobrym punktem wyjścia, żeby w ogóle spojrzeć inaczej na Apple.

[MARIUSZ] Tak, dokładnie! To tak naprawdę powinno być podstawowym zdaniem, podstawową frazą, który każdy powinien mieć w głowie, każdy menedżer powinien mieć w głowie, który używa sprzętu Apple. On powinien wiedzieć, jak jego dane są chronione i przez sam fakt, że nikt, ale absolutnie nikt nie może mieć dostępu do jego danych.

[KRZYSZTOF] Tak. I jakie dane teraz zbiera Apple. To oczywiście, moi kochani, nie jest tak, że my sobie to wymyśliliśmy, czy musieliśmy to konsultować z samym Apple, bo to są informacje publicznie i od tego bardzo chcę zacząć dzisiaj, dostępne. Gdzie są one dostępne? A no moi drodzy, to jest ta sama dyskusja, która być może przydałaby się panu administratorowi, który nie wie jak włączać magii, ale również przydałaby się każdemu i każdej z nas, którzy mamy lub chcemy mieć lub

nabywamy dopiero co pierwszy sprzęt Apple, a dyskusji opartej o to, że OK, ale gdzie ja mogę, czy Apple ma instrukcję obsługi? Czy ja mogę o tym poczytać gdzieś, przecież na tej stronie Apple to są tylko zachęty kup, kup więcej, więcej, wydaj więcej pieniędzy!? Jasne, ale na tych samych stronach Apple w domenie polskiej, moi drodzy, jest jakiś tuzin dokumentów przetłumaczonych na język polski, mających czasami po kilkaset stron, ale wygodne spisy treści i skróty również w sobie, które o wszystkich tych rzeczach mówią. Po pierwsze mówią o tym, jak obsługiwać każde z urządzeń, bo jest to wymóg unijny, te instrukcje obsługi muszą gdzieś być i są w internecie opublikowane.
I bardzo dużo rzeczy, o które pyta się na przykład na X, czy na innych portach społecznościowych ludzi, tak zwanych *fanboyów* Apple'a, można by znaleźć równie dobrze w instrukcji obsługi na stronie Apple. Bardzo fajnie obrazkowo nawet wytłumaczone. Ale nikt o tym nie wie, że te instrukcje tam są, prawie nikt…

Tak samo są kwestie związane z prywatnością. Dokumenty, które są podlinkowane w opisie do tego odcinka, mówią o tym właśnie, jak Apple zbiera i przetwarza dane, I dla przykładu z jednego z tych dokumentów, z takiej jakby takiej biblii o prywatności, możemy się dowiedzieć, że dane osobowe wspierane przez firmę Apple od użytkownika to są dane w postaci informacji o koncie, o urządzeniu, danych kontaktowych do tej osoby, informacje o płatnościach, transakcjach, informacje dotyczące zapobiegania oszustom, dane z użycia danych urządzeń, dane z informacją o lokalizacji, o zdrowiu, o sprawności fizycznej, no bo tam jest w końcu Apple Health, dane do dokumentów tożsamości itd. Ale uwaga, to nie oznacza, że wszystkie te dane są odkryte dla Apple'a. Większość tych danych nie jest w ogóle odkryta, są to dane zanonimizowane. Potrzebne owszem do rozwijania usług i floty usług w ogóle całych Apple, na przykład Apple Fitness, ale nie po to, żeby te dane w żaden sposób sprzedawać, ani w żaden sposób je podglądać. I dlatego też dane osobowe trzymane przez Apple na urządzeniach użytkowników są trzymane, na urządzeniach. I to jest clue: Tak zwana bezpieczna enklawa, Secure Enclave, o której mogliście słyszeć.

To jest właśnie to fizyczne miejsce na urządzeniach, już w tym momencie wszystkich, gdzie te dane są trzymane i do niej wjazd macie tylko Wy, bo tylko Wy znacie swoje hasła dostępu, o nich jeszcze zaraz sobie powiemy, lub jesteście w stanie się zalogować do danych usług aplikacji biometrii. Coś byś tutaj dodał jeszcze z punktu widzenia tych swoich wdrożeń?

[MARIUSZ] To jest niesamowita sprawa. Dlatego, że bardzo dużo użytkowników pyta się tak naprawdę, co to oznacza, że te dane są trzymane i jak te dane są trzymane. Bardzo wielu osobom zdaje się, że ten odcisk palca to jest taki skan. które urządzenie robi i gdzieś tam sobie ten skan przechowuje. Absolutnie nie. To nie jest żaden skan, to nie jest żaden obrazek. I to jest fenomen tego urządzenia. To urządzenie tłumaczy ten skan na zapis matematyczny. Tak samo jak się dzieje zresztą z odbiciem naszej twarzy, Face ID. To również jest tłumaczone na język matematyczny i w postaci właśnie matematycznej zewnętrznej jedynkowej jest to zapisane w bezpiecznej strefie, właśnie Secure Enclave, o której powiedziałeś, która mało tego, ona jest jeszcze dodatkowo zabezpieczona swoim własnym, niezależnym procesorem, który właśnie się nazywa Securing Enclave Processor. Więc niesamowita sprawa i to jest zupełnie wydzielone od dysku, w którym takie urządzenie dysponuje.

[KRZYSZTOF] Czyli od procesora głównego, żeby to powiedzieć. To jest tylko jedna z jego składowych.

[MARIUSZ] Tak, to troszeczkę tak. Ja bym użył takiego porównania: wyobraź sobie, że masz w domu sejf, w którym trzymasz swoje kosztowności, ale do tego sejfu nie możesz się tak prosto dostać. Co musisz zrobić? Wezwać specjalnego technika, specjalnymi poświadczeniami, który ciebie zweryfikuje, że ty to ty.

[KRZYSZTOF] Ciekawe porównanie.

[MARIUSZ] I on ci pozwoli do tego sejfu wejść. To jest do tego stopnia bezpieczne.

[KRZYSZTOF] Tak, i dobrym przykładem tego jak to rzutuje, jak obecność tej bezpiecznej enklawy na całą platformę i tu mam na myśli całą platformę, czyli wszystkie możliwe platformy systemowe i sprzętowe.

Jest ostatnia sytuacja z CrowdStrike, z piątku zeszłego, kiedy to nagrywamy, kiedy po prostu wysadziło bluescreeny, nie z winy do końca Microsoftu, ale na ogromnej flocie urządzeń na całym świecie i sparaliżowało lotniska, służby medyczne, etc., bo po prostu nie ma tam czegoś takiego, co u Apple nazywa się Apple Endpoint Security Framework. Już tłumaczymy o co chodzi. Czyli wprowadziła go macOS Catalina, z tego co dobrze pamiętam, i to umożliwia monitorowanie zdarzeń związanych z bezpieczeństwem bez naruszania prywatności użytkowników, żeby zapobiegać na przykład wdrożeniu takich wadliwych aktualizacji *vendorskich*, jak ta

w przypadku CrowStrike, które by wysadziły, mówiąc zupełnie wprost w kosmos, całą flotę MDM. Maców, iPhone'ów, czegokolwiek i doprowadziły do tego, co obserwowaliśmy w piątek w przypadku wybranych kilku milionów urządzeń od konkurencji. Dlaczego tego nie ma? Microsoft się tłumaczy, że nie może tego zaimplementować, bo są regulacje unijne, ale ja zawsze sprowadzam tę dyskusję do punktu zero. Punkt zero to jest – prywatność jest podstawowym prawem człowieka! My nie powinniśmy w ogóle się zastanawiać kto co może wprowadzić, bo to już powinno być wprowadzone. Może to jest naiwne myślenie, ale u Apple tak jest.

[MARIUSZ] I to działa. I to działa.

[KRZYSZTOF] W sensie tam nie ma możliwości, żeby się taki błąd zrobił, bo po prostu architektura na styku software, hardware nie dopuści do scenariusza, który by ją wywołał. To jest niesamowite i bardzo wyraźne po ostatnim piątku.

[MARIUSZ] Oj, to prawda. Tak to właśnie wygląda w przypadku Apple, bo nawet na poziomie *software'owym* Apple ma przy tych swoich urządzeniach mechanizmy, które dbają o to, że oprogramowanie, które jest wgrywane na te urządzenia, jest zgodne. Tutaj nic nie ma prawa się wysypać.

[KRZYSZTOF] Właśnie, bo z punktu widzenia Twoich MDM-ów też możesz powiedzieć, że jak rozumiem też Apple szkoli, czy to Was jako iMAD, jako wdrożeniowców później, czy w ogóle osoby, które się tym zajmują, w kontekście tego, jak wytłumaczyć organizacji, która przechodzi na flotę nadgryzionych rzeczy, wytłumaczyć to, jak oni się mogą zabezpieczyć? Żeby te aktualizacje były częste, no bo to jest w końcu świat Apple, ale też, żeby były bezpieczne. Takie mechanizmy, jak przypuszczam, istnieją i są do tego całe procedury.

[MARIUSZ] Oczywiście, że tak! Mamy mnóstwo rozwiązań w zakresie MDM, a są takie środowiska właśnie MDM-u, czyli Mobile Device Management, które bardzo ściśle współpracują z samym vendorem, z Apple. I skutek jest taki, że te rozwiązania, które są prowadzone na rynek, one są bardzo, ale to bardzo spójne z kolejną aktualizacją macOSa, iOSa i tak dalej. W związku z tym w wielu przypadkach nie ma potrzeby takiego okresu karencji, w której to administratorzy musieliby sprawdzić, przetestować, czy to, co zamierzają wprowadzić w firmie, będzie działać.

[KRZYSZTOF] I to jest szalenie ważne, bo to się wydaje standardem gdzie indziej, że no okej, jest coś nowego, ale to zanim to w ogóle obsłużymy, to poczekajmy, się uleży i tak dalej. Tu nie ma takiego myślenia.

[MARIUSZ] Tutaj takie rozwiązanie mogło być wprowadzone w wielu przypadkach niemal od ręki. To daje niesamowite poczucie bezpieczeństwa właśnie administratorom, czy też użytkownikom tego sprzętu.

[KRZYSZTOF] I też w ogóle aktualizacje częste i automatyczne to jest coś, co wyróżnia Apple. To jest kolejny punkt. W sensie, to też pokazuje wiele badań rynku. Przykład jesieni. Wchodzą nowe systemy. To Apple ma adopcję nowych systemów na rynku na poziomie 70%? Nie wiem, dwa tygodnie po premierze nowego iOS-a, czy nowego iPadOS, czy nowego macOS to jest nieosiągalne.

[MARIUSZ] Muszę się przyznać, że sam jestem już użytkownikiem wersji beta…

[KRZYSZTOF] To jest szaleństwo, ale to jest inna sprawa, bo ty jesteś *fanboyem* <śmiech>. To też jest taka kalka śmieszna, ale znajdź mi kogoś, kto czeka, aż wyjdzie publiczna beta u konkurencji i ją testuje. To jest prawda, to się zgadzam.

Ochrona dostępu do iPhone'a. I tutaj warto powiedzieć, że sam iPhone w jakiś sposób się zabezpieczy, ale bez dobrego hasła czy bez włączenia dwuskładnikowej weryfikacji natywnie wymuszanej przez Apple. To też jest szalenie istotne. Jak sobie konfigurujemy pierwszego Maca czy iPhone'a czy cokolwiek innego, nawet zegarek, to one nas proszą, te systemy, ustaw kod dostępu, ustaw hasło, zacznij używać Touch ID albo Face ID. Możemy to pominąć, ale domyślnie jest to wymuszane.

[MARIUSZ] I tutaj moja drobna sugestia. W ramach ustawienia kodu do iPhone'a warto jednak korzystać z haseł alfanumerycznych.

[KRZYSZTOF] Tak jest! Ja mam po prostu ustawione zdanie, które tylko ja pamiętam, z różnymi kombinacjami wielkości liter, etc. To jest dobry kierunek, słuchajcie, to jest dobry kierunek, to jest najtrudniej też złamać, natomiast pamiętajcie, że to jest jedno i to samo, tak jak Mariusz powiedział, czyli ustawiając sobie alfanumeryczne mocne hasło, macie też mocne Face ID czy Touch ID. Dlaczego? Dlatego, że to jest i tak reprezentacja tego hasła. W uproszczeniu, nie? W dużym uproszczeniu, ale jest. To nie jest obrazek dodatkowy, to nie jest zdjęcie Twojej twarzy, jak bywa u konkurencji, którym jesteś w stanie odblokować, nie? To

jest po prostu odpowiednik tego hasła, które ustawicie, więc jakby to jest szalenie istotne, żeby to hasło było mocne też.

[MARIUSZ] Wspomniałem o tym haśle alfanumerycznym chociażby z tego powodu, że w Stanach Zjednoczonych były albo są dość popularne takie modele kradzieży, które polegają na tym, że użytkownik jest podglądany w momencie wprowadzenia swojego kodu, cztero albo sześciocyfrowego, tak jak najczęściej to jest. I w tym momencie następuje przechwycenie tego iPhone'a, prawda? Złodziej po prostu pamięta ten kod, no bo cztery albo sześć cyfr jest raczej proste zapamiętania. I co w tym momencie się dzieje? No w tym momencie on natychmiast zmienia ustawienia w naszym prywatnym Apple ID. Tak naprawdę robiąc nam szkodę niewyobrażalnych rozmiarów, no bo tak naprawdę ile kosztuje nasze życie cyfrowe, a najczęściej to nasze życie jest ukryte w naszych urządzeniach. W naszych komputerach.

[KRZYSZTOF] Tak, nawet w naszym zegarku.

[MARIUSZ] Tak, dokładnie!

[KRZYSZTOF] Są już przypadki, że ktoś zrobił na kimś, wyzerował mu konta bankowe, bo ktoś miał zegarek i jakby nie zabezpieczył go. Są takie przypadki i da się to zrobić. Więc trzeba mieć świadomość, że w chorych czasach żyjemy, a z drugiej strony nie będzie lepiej. Więc zastanówmy się na drugi raz, jak wchodzimy do komunikacji miejskiej i robimy przelew natychmiastowy z naszego banku, nie mając żadnego filtra polaryzacyjnego naklejonego na nasze urządzonka, i robią to po prostu swawolnie pod kamerami przedsiębiorstwa komunikacji, pod ludźmi, którzy stoją nad nami i się trzymają po prostu rurki…

[MARIUSZ] Ja sobie właśnie wyobraziłem chyba jeden z najgorszych scenariuszy, tak mnie natknąłeś ku temu, mianowicie wyobrażam sobie tę osobę, która ma bardzo prosty kod dostępu, tym kodem dostępu odblokowuje swojego iPhone'a siedząc w kawiarni z ogólnie dostępną siecią Wi-Fi, niczym nie zabezpieczoną i w tym momencie robi przelew.

[KRZYSZTOF] Na przykład, nie? I jakby dlatego to jest ta słynna dyskusja, dlaczego ja mówię, kupujcie, jak już chcecie kupować iPada i na nim gdzieś pracować jako o mobilnym komputerze, kupujcie iPady z LTE. Miejcie swój internet, nie? Nie

korzystajcie, nie polegajcie tylko na VPN-ach, bo VPN-y też można złamać i VPN-y też są zawodne, nie. Nawet na macOS.

[MARIUSZ] Albo przynajmniej sparujcie tego iPada ze swoim iPhone'em, prawda? Korzystajcie z sieci, którą iPhone dostarczy.

[KRZYSZTOF] Dokładnie tak. Dalej, kontrola bezpieczeństwa.

To jest w ogóle taki ogromny moduł cały tak naprawdę, szczegółowo opisany w bardzo długim dokumencie (po polsku), który mówi nam o tym, co to znaczy, że możemy ustawić zaufany kontakt do odzyskiwania konta Apple ID. W czym nam taki kontakt pomoże, a w czym nam może przeszkodzić i w jakich scenariuszach. Jak możemy sprawdzić, kto ma dostęp do naszego iPhone’a lub iPada lub sami zdecydować, komu ten dostęp damy, kiedy na przykład ten telefon zgubimy lub kiedy na przykład nie będziemy mogli go obsłużyć, bo to też jest scenariusz, który może się wydarzyć. A warto to robić, bo wypadki chodzą po ludziach.

[MARIUSZ] Oczywiście, że tak. Zwróćmy też uwagę, że nasze urządzenie, nasz iPhone, iPad czy Mac w momencie odpalenia jakiejś aplikacji, która niesie sobie korzystanie z jakichś danych wrażliwych, ona się pyta, czy to urządzenie jest urządzeniem zaufanym, wysyła nam kod do odblokowania. To są niezwykle ważne rzeczy, na które trzeba zwracać uwagę.

[KRZYSZTOF] Tak, i to weryfikowanie, kiedy się logujemy Apple ID, w jakikolwiek sposób drugim urządzeniem spiętym z tym kontem, jest niesamowite i dostępne tylko tak naprawdę na tej platformie. Jako nie wdrożenie dla instytucji czy korporacji, ale dla zwykłych ludzi. No nie wiem, mam po prostu nowy telefon, to zanim się do niego w ogóle dostanę, muszę się zweryfikować, tak? Na innym urządzeniu, które już mam wspięte z Apple ID, odczytać tamten kod, nie wiem, użyć kombinacji klawiszy na zegarku, cokolwiek, nie. Ale zrobić to.

My teraz mówimy o takim skrajnym scenariuszu dodawania nowego urządzenia, ale to się nawet pojawia przy zakupach filmów Apple TV, gdzie musisz to potwierdzić na iPhonie dwuklikiem, żeby obciążyło twoją kartę. I taka magia, o której się dużo mówi, że w Apple'a jest dużo rzeczy takich niewidocznych. No to jakbym miał wskazać jeden silos, to by była prywatność. To jest największy silos, gdzie są rzeczy niewidoczne dla Kowalskiego czy Smitha, magiczne i które go chronią. Właśnie ten silos bym wskazał w całej magii Apple'a.

[MARIUSZ] Tutaj jeszcze a propos tego, co mówisz, można później co dalej i też zapoznać się z takim tematem, który nazywa się ochroną skradzionego urządzenia. To a propos tego, o czym przed chwilą mówiliśmy przed chwilą rozmawialiśmy, to jest kolejna funkcja Apple, która została dość niedawno wprowadzona. Astro, naprawdę warto się zapoznać właśnie, żeby uniknąć takiej sytuacji, że ktoś czyta nasz kod, który właśnie wprowadzamy do naszego iPhone'a. Apple też o tym pomyślało. Warto wiedzieć, że coś takiego istnieje.

[KRZYSZTOF] Tak, i że ta ochrona skradzionego urządzenia, kiedy jest włączona, to pozwala nam tak naprawdę bardzo szybko zablokować dostęp nawet do całego Apple ID, a w kooperacji z kontrolą bezpieczeństwa, na przykład z posiadaniem kontaktu zaufanych, później. odzyskać to Apple ID, kiedy przyjdzie na to czas, na przykład po powiadomieniu i współpracy z policją, a nie utracić go na zawsze, tak jak to było dawniej.

I cała ta sprawa kodami to wypłynęła dzięki The Wall Street Journal i Joanny Stern, która porozmawiała z ofiarami tak zwanego tak zwanych kradzieży na podglądacza i to jest tak jak Mariusz mówi, ci ludzie stracili dużo ze swojego, jak nie całe swoje cyfrowe życia, a bardzo często stracili też coś więcej i nie chcecie być na ich miejscu. Tak jak mówiłem na początku też, że logiczne myślenie. Nie róbcie tych przelewów komunikacji na litość i też włączajcie te wszystkie rzeczy, które można i które Apple daje jako jedyne bardzo często. Bo zawsze w tym przypadku lepiej mieć to włączone niż nie. Prawie zawsze oczywiście, ale tak to jest.

[MARIUSZ] I tutaj przechodzimy do jeszcze jednej rzeczy, pewnie o której będziemy za chwilkę rozmawiać, mianowicie – kwestia backupu. Ile wart jest nasz backup? I tutaj zawsze się śmieję, nawet u swoich najbliższych miałem taką oto sytuację, że czy ja muszę dopłacać te 5 zł po to, żeby mieć te 50 GB w iCloud. No to zastanów się proszę, ile warte są twoje wspomnienia, dane, zdjęcia, to wszystko co przechowujesz, a co tak naprawdę należy backupować?

[KRZYSZTOF] Tak i ja pamiętam, że jak miałem też współpracę z Synology, to poznałem w ogóle całą załogę, i wtedy sobie kupiłem jeszcze NASA. To jest oczywiście scenariusz *hardcore'owy*, że ja jeszcze backupuję to, co jest backupowane w iCloudzie na prywatnym serwerze. To jest jasne, to trzeba być świrem, ale właśnie dlatego, że to jest bezcenne.
[MARIUSZ] Tak, bezcenne. Oczywiście!

[KRZYSZTOF] A jeżeli chodzi o takie kopie dla wszystkich, to ja zawsze zachęcam, żeby robić oprócz kopii iCloud kopię lokalną. Na macOS możecie sobie podłączyć iPhone'a i iPada i przez Findera zbackupować sobie zawartość jako lustrzany obraz dysku tych urządzeń do waszego Maca. Warunek brzegowy? No trzeba mieć wystarczającą ilość miejsca na tym Macu, dlatego może nie zawsze dobrym pomysłem jest kupowanie 256 GB dysku. Ale da się to też obejść. Ja na łamach iMagazine opisywałem, jak sobie wysłać taką kopię lokalną na zewnętrzny dysk, na przykład podpięty do Maca. Da się to zrobić.

[MARIUSZ] Bardzo polecam to rozwiązanie!

[KRZYSZTOF] Co to daje? To daje, że jak sobie zmieniacie ten swój telefon, to potem przywracacie go 1 do 1, do momentu, w którym został wykonany taki lokalny backup. Nawet z tym, gdzie był kursor zatrzymany w notatkach. I ja tak zawsze robię. Ja wolę przywrócić cały obraz dysku i to, co jeszcze brakuje, to sobie ewentualnie, jeżeli chodzi o dane aplikacji trzeciej, sobie tam dociągną te aplikacje po przywróceniu. Natomiast lwia część jest przywrócona 1 do 1. I dzięki temu, że mamy teraz USB-C czy wsparcie dla Thunderbolt, gdzieś to w kilkudziesięciu minutach, błyskawicznie, a nie w godzinach, jak to czasem bywa przez iCloud lub jak macie słabszy net lub jak to dawniej bywało przez Lightning. No, więc korzystajcie z tych lokalnych backupów, bo to jest złoto, nie. Do tego taki backup można jeszcze dodatkowo kryptograficznie zaszyfrować dodatkowym hasłem, tak zwanym hasłem backupu z poziomu macOSa, co też warto oczywiście zrobić. To tak, żeśmy powiedzieli, myślę, że to ważne. Ja jestem orędownikiem tych backupów.

[MARIUSZ] Wszystko co dotyczy bezpieczeństwa jest niezwykle ważne, tym bardziej, że są to bardzo proste rzeczy do zrealizowania.

[KRZYSZTOF] Bank haseł, to jeszcze trzeba powiedzieć. Na jesieni debiutują nowe systemy z natywną aplikacją Hasła, ale do tej pory mamy Keychain, czyli Pęk Kluczy. Mamy obsługę haseł w Safari i w ogóle globalną w systemie. Zapisujcie sobie te hasła i ustawiajcie hasła mocne, system już sam, dowolny system jest w stanie Wam wygenerować mocne hasło, jak mu na to pozwolicie i nie wybierzecie, ustawię sobie sam i nie piszemy tam Asia141, no to będzie generalnie bezpiecznie i dlatego takie rozwiązania natywne, są tak bardzo wymuszane przez Apple.

Zauważ, że Safari jako jedyna przeglądarka na świecie w tym momencie, nawet był ostatnio o tym fajny spot reklamowy, jest na tyle bezpieczna, że po prostu tak, nie jestem z latającymi kamerami jak kuki, nie? I fajny spot w ogóle, jeden z najlepszych, jakie Apple chyba zrobiło w ostatnich latach. Kreatywny taki, w sensie nieprzekombinowany.

Safari nie czyta tego, co przeglądacie w sieci. Ale też Safari jako pierwsze było to przeglądarką, która tak uparcie wymuszała ustawię Ci silne hasło. Ustawię Ci silne hasło. Warto z tego korzystać. Naprawdę. A to jest super.

[MARIUSZ] Ja w ogóle muszę Ci powiedzieć, już dawno pozostawiłem właśnie przeglądarce Safari czy w ogóle aplikacjom ustawienia haseł. Raz, że wiem, że te hasła są po prostu bardzo mocne. Dwa, kto by chciał pamiętać setkę albo więcej haseł do każdej aplikacji, do każdego portalu. To jest niepotrzebne, dlatego naprawdę odradzam i chyba czas zakończyć zapisywanie haseł na różnych kartkach, notatnikach i tak dalej, i wertowanie tego wszystkiego. Urządzenia Apple robią to doskonale, chociaż muszę Ci powiedzieć, że hasła alfanumeryczne, jakkolwiek bardzo mocne, są nadal hasłami w jakiś sposób po prostu zapisywanymi. W tej chwili coraz większą popularnością cieszy się tak naprawdę logowanie za pomocą kluczy publicznych i prywatnych. I to jest to, co Apple bardzo mocno wspiera. I to myślę, że to jest w ogóle superbezpieczna technologia, bo ona tak naprawdę pozbawia nas albo raczej czyni tworzenie jakichkolwiek haseł zupełnie niepotrzebnym. To jest zupełnie inny sposób logowania i większość już tych dużych firm na taki sposób logowania pozwala, na przykład Google chociażby.

[KRZYSZTOF] Tak i w ogóle to jest ta sytuacja, w której dajecie zaloguj się z uwierzytelnieniem klucza lub zaloguj się przez Apple ID i ono wyświetla na Mac OS taki monit, czy się zalogować, kontynuuj. I jeżeli jesteście zalogowani do swojego systemu albo macie na nadgarstku Apple Watcha, żeby to poświadczyć jeszcze, to tam nie ma żadnego wpisywania. Tam jest tylko jedno poświadczenie, tak zaloguj i tyle. I system za Was tak naprawdę poświadcza, za Was się dzięki tym kluczom loguje i dba, żeby to było bezpieczne.

[MARIUSZ] A znów klucz do logowania jest przechowywany na naszym urządzeniu. On nigdzie nie wypływa.

[KRZYSZTOF] Dokładnie, w naszej bezpiecznej enklawie.

[MARIUSZ] Więc jeżeli witryna pokazuje ten klucz publiczny, to tego klucza publicznego pasuje tylko ten klucz, który jest przechowywany na tym konkretnym urządzeniu.

[KRZYSZTOF] Klucz deszyfrowujący, bo nim mówimy, tak jest.

[MARIUSZ] Tak, dokładnie. On jest przechowywany na urządzeniu, którego nikt nie ma prawa poznać.

[KRZYSZTOF] Nawet samo Apple. Tak, bo ono nie widzi tego klucza. Ten klucz jest lokalny. On jest na Waszym urządzeniu trzymany. I teraz uwaga! To nie ma znaczenia, że Apple ID jest jedno na kilku urządzeniach. Bo każde urządzenie poświadcza tak naprawdę Wasze logowanie, czyli poświadcza Was swoim kluczem. Swoim własnym kluczem, tak. I to jest szalenie istotne i myślę, że wyróżniające w kolejnym punkcie całą tę firmę.

Dalej.

Oczywiście takie rzeczy jak zarządzanie informacjami, które udostępniamy aplikacjom, czyli przywileje aplikacji, no to są jeszcze czasy albo próbę podjęto wtedy w tych czasach Windowsa Visty. Nieudaną próbę. Apple zrobiło to mądrzej i Apple zrobiło to też w taki sposób, żeby trochę idioto-odpornie chronić tych użytkowników, nawet jeżeli zignorują te pop-upy.

[MARIUSZ] I na to bym też zwrócił uwagę. Masz absolutnie rację, bo jakkolwiek Apple chroni tę naszą prywatność, to Apple też nam w jasny sposób pokazuje, jak firmy dostawcy aplikacji chcą korzystać z naszych danych. Więc za każdym razem, kiedy instalujemy jakąś aplikację z App Store, no to ta aplikacja jasno nam ma obowiązek powiedzieć i mówi, co z jakich naszych zasobów ona będzie korzystała. Warto się zapoznać z takimi rzeczami, warto to po prostu czytać.

[KRZYSZTOF] Tak jest i to jest na karcie każdej aplikacji w App Store, na każdej platformie systemowej już jako obowiązek po stronie deweloperów wyszczególnione. Więc jeszcze zanim klikniecie kup lub pobierz, możecie wiedzieć do czego dostęp będzie mogła mieć ta aplikacja, jeżeli jej na to pozwolicie lub zapoznać się z informacją, co kiedy odmówicie tego dostępu, bo może się okazać, że nic, bo aplikacja nie będzie w stanie w ogóle wykonywać swoich funkcji. I Apple wymusiło jako pierwsze, żeby deweloperzy to opisywali. To Apple to wymusiło. Z

dużą ich niechęcią, przyznaję. Tak, tak, to prawda, to prawda, z dużą ich niechęcią. Blokowanie mechanizmów śledzących w Safari, to już powiedzieliśmy, szyfrowanie end-to-end, FaceTime i iMessage, szalenie istotne, a wkrótce również o obsłudze RCS-ów, nie?

[MARIUSZ] Ja bym powiedział jedno: zielone jest, może inaczej, niebieskie jest OK, zielone jest czerwone. Gdzieś to przeczytałem. Bo to nam mówi, kiedy nasze wiadomości są szyfrowane. iMessage jest szyfrowany, o czym świadczy, mówiąc najprościej, ten niebieski kolor naszych wiadomości. Co oznacza, że tak naprawdę ta wiadomość jest zaszyfrowana od początku do końca. Kiedy opuszcza nasze urządzenie i cały czas do momentu przeczytania tej wiadomości przez odbiorcę, bo tak naprawdę dopiero wtedy jest odszyfrowana. To ma dużo znaczenia, ponieważ wiele osób tak naprawdę nie wie, na czym polega to szyfrowanie i nie wie, na czym polega różnica w szyfrowaniu, jeżeli tak to można nazwać, między iMessage, a między na przykład zwykłym SMS-em?

[KRZYSZTOF] Nie wie, i tu się zgodzę, natomiast postawię przecinek, ale nie musi Mariusz wiedzieć i nie powinna musieć wiedzieć i to jest właśnie realizowane przez Apple. W sensie w sposób jeszcze ułomny, bo można to lepiej było zrobić i teraz będzie na przykład na jesieni dyskusja, ok, wejdzie obsługa RCS, czyli tego standardu, który pozwoli na reakcję, co już dawno powinno być zaimplementowane w iMessage na reakcję pomiędzy różnymi urządzeniami. Kiedy użytkownik Androida wysyła coś do użytkownika iOS i ten chce mu dać łapkę w górę No i super. De facto RCS będzie też szyfrowany end-to-end. Ale ponieważ nadal pozostanie ten bąbelek zielony, to użytkownik końcowy nie będzie wiedział, chyba że da łapkę, że to jest RCS, a niezwykły SMS? I to nie jest rozróżnione. To jest dziwne. Tak sobie ostatnio o tym myślałem. Więc jeszcze tu można by było zrobić lepiej, ale ogólnie, jakby to nie dzieliło społeczeństwa w Stanach, to ludzie się sądzić chcą o to. Tak jak Mariusz powiedział, niebieskie jest szyfrowane zawsze. I myślę, że dlatego Apple się z tego rozróżnienia kolorami nie będzie chciało wycofać.

[MARIUSZ] Nie, nie sądzę. Tutaj też trzeba pamiętać o tym, że jakkolwiek nasze dane są szyfrowane, to one nie są szyfrowane, przynajmniej nie wszystkie, w momencie tworzenia backupu w iCloud. Na to też trzeba zwrócić uwagę, to ma swoje uzasadnienie w takich sytuacjach, powiedzmy sobie, naprawdę skrajnych, krytycznych, kiedy ktoś w jakiś sposób musi mieć z przyczyn oczywistych dostęp do naszego backupu. I wtedy Apple, widząc, że ten backup nie jest szyfrowany, może udzielić takiego dostępu. Ale… to też może być zablokowane, ponieważ w

iPhone mamy taką funkcję zaawansowaną ochronę danych. I po włączeniu tej funkcji nasze dane na iCloud, te dane backupowane, również są szyfrowane i również Apple nie ma do nich dostępu. To jest niezwykle istotne, żeby rozważnie korzystać z tej funkcji, dlatego że w takim wypadku nie mając, nie pamiętając zagubiwszy hasło dostępu do naszych danych, nikt nie będzie w stanie ich otworzyć.

[KRZYSZTOF] Tak, takie hasło można sobie albo klucze awaryjne podrukować również i fizycznie schować w jakimś miejscu, o którym tylko my wiemy oczywiście też, ale jeżeli się tego nie zrobi i się zapomni, to będzie tak jak Mariusz powiedział, dodatkowym punktem jest tutaj znowu powrót do tego ogromnego silosa, czyli kontrola dostępu. Jeszcze raz, jakbym miał wskazać jakiś jeden dokument z linków w opisie tego odcinka, z którym warto się zapoznać, choćby go czytając kilka tygodni, to to jest ten dokument i to jest również część kontroli dostępu, a mowa tutaj o kontakcie zaufanym. Jeżeli włączymy zaawansowaną ochronę iCloud i mamy ustawiony kontakt zaufany, to jeszcze w ten sposób możemy sobie pomóc, ale będzie to też wymagało wieloetapowej weryfikacji na urządzeniach tego kontaktu zaufanego, żeby nam w ogóle pomóc. Natomiast jest to furtka, ale mało osób będzie o tym wiedzieć.

[MARIUSZ] Jest to furtka, też pamiętajmy o tym i uspokójmy niektórych słuchaczy, że ustawienie takiej osoby zaufanej nie oznacza, że ta osoba zaufana ma dostęp do naszych danych. Absolutnie nie! Ona ma tylko dostęp, znaczy poda nam tak naprawdę kod dostępu do naszych urządzeń, nic więcej.

[KRZYSZTOF] Dokładnie.

Dostęp do mikrofonu, kamery, lokalizacji i ta słynna lampeczka na każdym urządzeniu, obok Dynamic Islands, albo w ramach Dynamic Islands lub obok Notcha i na paseczku na górze w macOS, mówiąca nam: Słuchaj, korzystasz z mikrofonu (czyli pomarańczowe), korzystasz z kamery (zielone) światełko! To jest coś, co Apple wprowadziło i teraz wszyscy inni to kopiują, a to jest tak oczywiste, tylko znowu. I tak i nie. Oczywiste dla lajka, nieoczywiste dla tego, kto trochę głębiej to *zresearchował* i wie na przykład, że zapalenie tej lampeczki na określony kolor jest wykonywane, uwaga, na kanwie bezpiecznej enklawy. To ona decyduje, czy to zapalić, czy nie. Nie główny procesor jakby, nie. Dlaczego? Żeby nie można było tego zhakować i żeby ktoś z zewnątrz nie mówił błędnie, czy ktoś nasłuchuje, czy nie. Zobacz, nawet takie szczegóły, Mariusz…

[MARIUSZ] Za każdym razem, kiedy słucham to coraz bardziej, mimo tych moich lat tego doświadczenia, zawsze mnie to fascynuje, o ilu rzeczach tutaj pomyślano i to są rzeczy tak proste w dostępie, nie wymagające żadnej jakiejś specjalistycznej wiedzy, po prostu klikasz i masz.

[KRZYSZTOF] A tak zaawansowane pod spodem, nie? To jest niesamowite. I znowu, realizujący ten scenariusz, że kurczę, twoim podstawowym prawem jest prawo do prywatności. Kropka. W sensie my ci to prawo chcemy zapewnić. Ty nie musisz wiedzieć jak. I dostarczyć w jak najprostszy sposób. Tak, oczywiście. To jest niesamowite.

Tak samo polecam korzystać z funkcji „Ukryj mój e-mail", czyli w ogóle z zakładania kont już teraz na większości stron przez Apple ID.

[MARIUSZ] Och, to jest super sprawa! To jest super sprawa, dlatego mówię, warto korzystać z tych rozszerzonych backupów i warto dopłacić tych parę złotych właśnie do tego, żeby ten backup mieć większy, bo z tym łączy się właśnie ta usługa iCloud+, gdzie dostajemy to, o czym dokładnie mówisz, funkcję ukryj mój e-mail. z której korzystam nagminnie. To naprawdę ułatwia mi sprawę, bo ja wiem po prostu, kiedy otrzymuję jakąś wiadomość mailową, to wiem z jakiego źródła ona jest, prawda. Po prostu nie mam śmieci w mailach.

[KRZYSZTOF] Tak, i tak samo znajdź mój na aplikacji, czyli nie tylko, ja się zawsze śmieję, nie chodzi o śledzenie swoich członków rodziny, bo zakładam, że jak ktoś komuś mówi, że ej, dodajecie do iCloud Family, to nie mówi mu tego w tajemnicy, bo przecież musi to doświadczyć na swoim iPhone'ie. Więc to jest taka dyskusja, która zawsze jest wyciągana gdzieś tam na eksie i rozbija się o to, że ktoś nie wie o czym mówi… No więc tak to już po prostu bywa w naszej banieczce. Natomiast samo to, że mamy jedną aplikację, jeden hub, gdzie możemy śledzić urządzenia, możemy śledzić osoby, możemy te urządzenia zablokować lub skorzystać z tej ochrony kradzieżowej.

[MARIUSZ] No ale wyobraź sobie, że najbliższa ci osoba ma tylko jedno urządzenie Apple i właśnie został zgubiony. I gdzie jest mój iPhone. To najczęściej są nerwy. Tak naprawdę i wtedy wyłączamy takie bardzo racjonalne myślenie, a wystarczy kliknąć na aplikację Find My, mamy wszystkie urządzenia i widzimy, gdzie ono może być.

[KRZYSZTOF] Prosta sprawa. No i to jest właśnie, ty powiedziałeś, to się wtedy wyłącza logiczne myślenie. I zobacz, nawet to jest zaadresowane w całym dużym worku pod tytułem jak robimy, że nasze sprzęty są najbezpieczniejsze na świecie. Prawda? To jest coś, co wyróżnia Apple'a też, że ta warstwa behawioralna jest tak bardzo brana pod uwagę w pewnych sytuacjach. Bardziej mamy wtedy do czynienia z psychologią, a nie z jakimiś ukrytymi talentami informacyjnymi.

Oczywiście można by tu sporo jeszcze mówić o HomeKit czy o HealthKit. Tak naprawdę wiecie, głupie zdrowie systemowe, nie głupie, nie głupie. Macie Apple Watcha, macie wagę inteligentną w domu. To wszystko jest już jakby wśród tych topowych producentów, na przykład Withings, którego wiem, że też dystrybuujecie w iMAD. Jest to wszystko zsynchronizowane, wspiera Apple Health. No i teraz, kurczę, i jest anonimowe.

[MARIUSZ] Jest zupełnie anonimowe, wiesz, ja też korzystam z HomeKita, jest to po prostu świetne rozwiązanie. Raz, że tak jak mówisz, moje dane są całkowicie anonimowe, ale tak? Ile razy zdarzyło się, kiedy wyjeżdżasz na urlop i nagle będąc 100-200 km od domu, ojej, ja chyba nie wyłączyłem telewizora, tak z gniazdka po prostu. I cóż, właśnie po to jest HomeKit.

[KRZYSZTOF] Też korzystam, chociaż oczywiście jeszcze HomeKit mógłby być bardziej smart. Natomiast to też trzeba mieć z tyłu głowy. Niektóre rzeczy u Apple'a nie są takie, jak my byśmy chcieli użytkownicy, że: *„O Boże, bo tam konkurencja trochę lepiej to działa, albo trochę ma więcej funkcji, albo ktoś tam coś pomyślał!”*. No, tylko, że zawsze trzeba to dzielić przez prywatność. Dlatego, że niektóre rzeczy w Apple wchodzą później lub nie wchodzą w ogóle, bo nie przechodzą testu, tak zwanego testu, można by się to powiedzieć, choć teraz to wymyśliłem, testu prywatności. Czyli nie realizują tego, że dane są fundamentalnym prawem klienta, w związku z powyższym ich nie ma, nie pojawiają się.

[MARIUSZ] I tutaj tak naprawdę mówimy o bezpieczeństwie aplikacji w App Store, jak one są weryfikowane, nim trafią w ogóle, nim mogą trafić do App Store, a to jest zupełnie inna sytuacja niż mamy do czynienia w innym popularnym markecie, w którym takie aplikacje możemy kupić. Ta ścieżka jest zupełnie inna, ale dzięki właśnie niej mamy absolutnie pewność, że te aplikacje są zweryfikowane, że są sprawdzone, że nic w nich nie jest podszyte, co mogłoby zaszkodzić naszemu cyfrowemu ja.

[KRZYSZTOF] Oczywiście, tam też błędy się zdarzają i wtedy wszyscy o nich czytają na portale przyciągnięcia Apple'a.

[MARIUSZ] No tak, ale z tego się robi takie wielkie halo, no bo jak często takie błędy się zdarzają, więc jak nawet się trafi, to trzeba głośno o tym powiedzieć, no ale umówmy się…

[KRZYSZTOF] Pamiętajmy też, że to jest weryfikowane przez ludzi, jeżeli chodzi o App Store. Jak sobie czytamy raporty, a co roku taki raport o bezpieczeństwie Apple wydaje, gdzieś na wiosnę, w tym roku też zresztą był i to oni podają dokładnie w liczbach, ile osób, ile aplikacji sprawdziło i ile udaremniło niedoszłych fraudów tak naprawdę przez dziwny kod. I to są zawsze liczby w żaden sposób nieporównywalne z konkurencyjnym marketplace'em, dlatego że tam jest rząd wielkości albo dwa wyżej, jeżeli chodzi o ilość tych udaremnień. Jeszcze sobie myślę, żeby powiedzieć, warto było o kwestii takiej, że nie wszystko złoto, co się świeci oczywiście, jak już tak rozpocząłem mimowolnie. No czyli oczywiście o tym, że jasne, odpowiedź na aferę podglądaczy kodu jest, powiedzieliśmy, że jest to zaawansowana ochrona iCloud, są to też cała kontrola dostępu i tak dalej, spoko. Można jeszcze więcej w tym temacie na pewno zrobić. Apple nie robi tego, bo nie ma pewnie swojego idealnego rozwiązania na to, ale jestem przekonany, że nad tym pracują. żeby jeszcze mimo tej wiedzy o kodzie nie dało się tyle zrobić z Apple ID, co da się obecnie. Natomiast oni nad tym robią, oni to pracują, komunikują na ten temat.

[MARIUSZ] Jestem o tym przekonany. Apple wychodzi z założenia, że w opuszczonym rynku rozwiązania naprawdę sprawdzone w tym zakresie, więc porównywanie do jednych procentów, że inni to mają, Apple jeszcze nie spokojnie. zaczekajmy, Apple na pewno, tak jak mówisz, nad tym pracuje i kiedy to zrobi, na pewno będzie to rozwiązanie bardzo zapracowane.

[KRZYSZTOF] Inni też, można powiedzieć, inni to mają, ale inni nie mają Secure Enclave, więc mają, nie mają, mają, nie mają, to jest zawsze ta dyskusja, Mariusz, mają, nie mają, więc wiesz, bo jakaś tam dodatkowa ochrona oparta o usługę Third-Party albo *vendora* kolejnego, z którym podpisujesz umowę kontra bezpieczna enklawa, to ja nie wiem, gdzie się czuję bezpiecznie, hm? Sytuacja znowu z piątku, mi się przypomina mimowolnie. Dobrze, to myślę, że tak, bo można by tu jeszcze oczywiście mówić o wielu rzeczach, np. o udostępnianiu haseł Wi-Fi gościom w domu. Takich prostych rzeczach, które się wydają oczywiste, a za tym stoi właśnie

to, że prywatność jest swoim fundamentalnym prawem człowieka, drogi kliencie, droga firmo, droga korporacjo, *whatever*. I to jest super. Natomiast też nie chcieliśmy już tego odcinka zrobić po prostu doktoratu, więc po to w jego opisie, jeszcze raz, pod adresem boczemunie.pl/341/ znajdziecie listę według mnie, według nas, najważniejszych dokumentów dostępnych po polsku w większości na stronach w domenie Apple, gdzie możecie sobie poczytać na spokojnie na ten temat edukować się, żeby na przykład, kiedy ktoś z Waszej rodziny Was zapyta: *„A co ten iPhone ma takiego lepszego?”*, móc na przykład konkrety podać.

I ja polecam to podejście. Wakacje są do tego idealne, bo jakże lepiej zainwestować swój czas, jak nie to, żeby dowiedzieć się czegoś więcej na temat bezpieczeństwa, na przykład na temat tego, jak lepiej intencjonalnie wykorzystywać technologię, żeby służyła nam, a nie my jej. W przypadku Apple jest o czym czytać, Mariusz, zdecydowanie.

[MARIUSZ] Tak! Jak się uśmiechnąłem, jakże często słyszałem pytania albo słuchałem pytań, a w czym ten iPhone jest lepszy. Co też świadczy o pewnym podejściu, ale nie będziemy teraz o tym mówić, bo znów otworzymy kolejny rozdział.

[KRZYSZTOF] A to nie podcast, który ma 4 godziny, choć takie są, ale to nie ten adres.

Słuchaj, cztery najważniejsze według mnie rzeczy i też pewnie według Ciebie możesz coś dołożyć również od siebie, o których warto zadbać. Moi drodzy:

1. Rzecz absolutnie fundamentalna, odkładając to, że prywatność jest waszym fundamentalnym prawem jako ludzi, czyli trzeźwe myślenie i uważność na to, co, gdzie i jak robicie z waszymi urządzeniami cyfrowymi. Wspomniane robienie przelewów w MPK.

[MARIUSZ] Absolutnie to prawda. Niezależnie od tego, jak doskonałe narzędzia dostarcza nam Apple, to pamiętajmy o tym, że na końcu jest człowiek i to człowiek podejmuje decyzje. Lepiej, żeby one były dobre.

[KRZYSZTOF] 2. Mocne hasła, najlepiej alfanumeryczne. To już wybrzmiało, myślę, bardzo, bardzo w tym odcinku.

3. Włączenie biometrii, a właściwie szerzej dwuskładnikowej weryfikacji wszędzie, gdzie się da, w każdej usłudze, nawet nie od Apple. Gdzie się da.

4. I bycie na bieżąco. I tu mam takie trzy rzeczy, które Wam mogą pomóc w byciu na bieżąco. Jest taka aplikacja Cyberalerty od załogi Niebezpiecznika. Polecam sobie zainstalować. Dostajecie po prostu powiadomienia, kiedy jest akurat jakiś zmasowany atak na przykład na wnuczka albo na fałszywą stronę banku jakiegoś przeprowadzany w Polsce. Myślę, że nie trzeba Niebezpiecznika nikomu przedstawiać. Aplikacja jest darmowa.
Alerty BIK, czyli Biura Informacji Kredytowej, polecam sobie to włączyć. Abonament na rok kosztuje bodajże coś około 20-30 zł i wtedy po prostu Biuro Informacji Kredytowej monitoruje i wysyła Wam co miesiąc powiadomienie, czy ktoś nie podejmował próby wyłudzenia czy wzięcia kredytu na Was.
A żeby to w ogóle nie było możliwe, choć mimo wszystko BIK polecam mieć włączone te alerty, to zastrzeżcie sobie PESEL. A możecie to zrobić kilkoma kliknięciami w aplikacji mObywatel.

[MARIUSZ] I pamiętajmy o tym, że kiedy na ikonce kółek zębatych na ekranie iPhone'a pali się cyfra 1 bądź 2, nie ignorujmy tego. To znaczy, że nasze urządzenie chce nam przekazać ważny komunikat.

[KRZYSZTOF] Czyli aktualizujmy drogi kliencie, drogi użytkowniku.

[MARIUSZ] Najczęściej tak.

[KRZYSZTOF] Mariusz, bardzo mi się przyjemnie z Tobą rozmawiało. Jeszcze na pewno kiedyś chciałbym zgłębić temat MDM-ów jeszcze bardziej, bo wiem, że będzie to pewnie wartością dla moich słuchaczy. No właśnie, moi drodzy. Z przyjemnością służę swoim wiedzą. Jeżeli chcecie się czegoś jeszcze dowiedzieć a propos wdrożeń, a propos być może bardziej skomplikowanych rzeczy – dajcie znać, tam gdzie zwykle.

To był 341 odcinek tego podcastu. Ja szalenie dziękuję Mariuszu jeszcze raz za Twoją ekspertyzę. My się słyszymy za tydzień standardowo.

Dobrych wakacji i dobrej edukacji w kontekście Waszej prywatności na platformach Apple życzę. Trzymajcie się!

[MUZYKA]

Raz jeszcze, na koniec, żeby nie umknęło. Przypominam, zostaw na Apple Podcasts lub na Spotify taką liczbę ⭐ gwiazdek, jaką uznasz za stosowną.

Do usłyszenia w kolejnym odcinku, a za dziś bardzo dziękuję.

[MUZYKA CICHNIE – KONIEC ODCINKA]