05.09.2025 r.

#408

TRANSKRYPT ODCINKA

Jak Synology postrzega cyberbezpieczeństwo?

Partnerem tego odcinka jest Synology Polska.

[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.

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

Zaczynamy.

[MUZYKA CICHNIE]

[KRZYSZTOF] Czołem Moi Drodzy! Witam w kolejnym odcinku 13. sezonu „Bo czemu nie?”. Dawno nie było tutaj załogi Synology, z których rozwiązań sam od lat korzystam, jak dobrze zresztą wiecie, więc myślę, że to jest dobry moment, aby powitać ich po raz kolejny, zanim wszyscy przepadniemy w temacie nowych iPhone'ów. Ale tym razem, dotykając tematu tworzenia kopii, zapraszam od nieco innej strony, absolutnie elementarnej, a zatem bezpieczeństwa Waszych danych, które przechowujecie na ich urządzeniach lub w ich usługach, albo będziecie to, mam nadzieję, robić.

Zanim zaczniemy, przypomnę, że wszelkie linki do osób, rzeczy i archiwalnych odcinków zrealizowanych z Synology, albo innych rzeczy, które dzisiaj tutaj padną, znajdziecie pod adresem boczemunie.pl/408. Tam również znajdziecie link do mojego newslettera, który wysyłam w każdą sobotę o poranku. Warto subskrybować, bo niebawem ogłoszenie daty premiery mojego e-booka, który będzie rozdawany tutaj właśnie, tylko i wyłącznie osobom, które zapiszą się na Substacku – pozostawiając adres e-mail – a będzie dotyczył tego, jak zapędzić

Waszą technologię do pracy dla Was, a nie pracować dla niej. To niebawem, także warto subskrybować.

A moim i Waszym gościem jest dziś ponownie Przemek Biel. Cześć, Przemku, witaj ponownie!

[PRZEMEK] Witam wszystkich serdecznie, cześć.

[KRZYSZTOF] Przemku, zanim przejdziemy oczywiście do dzisiejszego odcinka, naszego głównego tematu, to korzystając z faktu, że Ciebie tutaj w okienku mam i że jesteśmy właściwie w przededniu jesiennych premier Apple, bo to już 9 września, to podpytam, jak wrażenia, sięgając nieco wstecz, po WWDC, bo ten aspekt software'owy tutaj dla Was w Synology też jest niezwykle istotny i też wiem, że mocno się tam zawsze szykujecie na premiery nowych systemów, pod różnymi kątami i patrząc na różne wektory. No właśnie, jeszcze przed ich oficjalną premierą to taki ważny moment, bo znowu nowe nazewnictwo, rodzina 26, dużo zmian. Jak tam wrażenia ogólnie?

[PRZEMEK] Generalnie, jako firma to w zasadzie zawsze patrzymy na to, żeby nic nie zepsuli. Bo wiadomo, jak jest software development, to wprowadzając nowe rzeczy, często zdarza się coś zepsuć, a jeszcze nie wiedząc o tym, to jest najgorsze. Natomiast z punktu widzenia takiego mojego personalnego, zainstalowałem sobie na iPadzie tę nową wersję beta. Bo tak, na produkcyjnym telefonie tego nie robię. I nie wiem, dla mnie tam niewiele się zmienia. Wygląda to może trochę ładniej. Jest więcej zabawy z okienkami, można to zrobić. Ale czy to jest jakieś diametralnie inne? Możliwe, że przy 13 calach na iPadzie będzie miało to jakiś sens i to rzeczywiście zmieni sposób pracy z takim urządzeniem. Natomiast przy 10 calach nie jestem przekonany.

[KRZYSZTOF] Co ciekawe, bo na przykład dla mnie to jest totalna zmiana, ale ja też używam iPada do montażu jako komputera właściwie, bo go podłączam do Studio Display i w tej konfiguracji, to jakby te okna są już czymś, co można praktycznie powiedzieć jak macOS. Więc ja tutaj zmiany rozumiem totalnie, ale to, co powiedziałeś, że niewiele widać na pierwszy rzut oka, no bo jeżeli się, wiesz, jest osobą, która podchodzi utylitarnie do urządzeń, w sensie jako do narzędzi pracy, a ty taką chyba osobą jesteś. Ja zresztą już coraz bardziej też to podejrzewam, że ty nie będziesz sobie na nowo obkładał ikonek czy wprowadzał jakichś ogromnych rewolucji po instalacji iPadOS 26, więc no, trochę tak ma być z takim systemem też, nie, że on nie ma wywrócić ci urządzenia do góry nogami. Tylko w przypadku takich chyba osób jak my, no, wszystko zostanie na swoim miejscu, a jak ktoś będzie chciał te dodatki znaleźć i ich użyć, albo faktycznie jakieś sobie zmiany wprowadzić

w układach na ekranach czy tak dalej, no to sobie to zrobi, nie? Ale co do zasady, po restarcie, to chyba dobrze, że to wygląda tak samo, tak mi się wydaje, nie? Że to może też wynikać z tego.

[PRZEMEK] Tak, z ciekawych rzeczy, które zauważyłem, to chyba wprowadzili język polski do tej usługi Scribble, w sensie, że możesz rysikiem wpisywać w pole tekst, a on ci to rozpozna. Przez chwilę to testowałem, ale włączyłem sobie tę opcję, bo wcześniej była domyślnie u mnie wyłączona, bo po prostu to po polsku nie działało i nie miało większego sensu. Teraz zobaczę, czy to w jakiś sposób poprawia produktywność.

[KRZYSZTOF] A powiedz mi, czy z punktu widzenia zmian na przykład w Safari? Bo tam trochę zmian jest, albo zmian w ogóle związanych z Liquid Glass. Was to jakoś dotyka, choćby w interfejsach webowych, które wyświetlacie, czy to w ogóle jest, jakby, w tym roku akurat nie wpływa na was? Tak, wiesz, na dużym poziomie ogólności.

[PRZEMEK] Wydaje mi się, że nie wpłynie to, o ile będzie to zgodne z jakimiś tam standardami, a w większości przypadków oni mają ten, ten, ten silnik na tyle zgodny, że za, za wiele nie psuje, tak? Bo wiadomo, wszyscy optymalizują strony pod, pod Chrome'a, bo tam największy udział w, w rynku, natomiast czasami na Safari coś wygląda inaczej albo coś nie działa, ale w tym przypadku, jak ja testuję nasze aplikacje na Safari, to w większości to spokojnie działa.

[KRZYSZTOF] Super, no to dobrze słyszeć też, że tutaj jest jakby wszystko klarowne. A powiedz mi, planujesz jakieś zmiany sprzętowe? Jeszcze tak krótko, tej jesieni, czy to nie jest Twój rok wymiany?

[PRZEMEK] Mój rok wymiany jest... Obecnie już jestem na takim etapie, że rzeczywiście podchodzę do tych sprzętów jak do narzędzi i póki wszystko działa, to po prostu nie widzę większego sensu. Mam jeszcze... Ja mam iPhone'a akurat w miarę nowego, mam piętnastkę, więc spokojnie jeszcze dwa, trzy lata to pociągnie. iPad jest tak używany pobocznie, więc i to jest Pro na M1. Więc no, a ewentualnie MacBook M1 Pro, natomiast też spokojnie jeszcze 2-3 lata pociągnie.

[KRZYSZTOF] No, ja 3 mu jeszcze celuję, tak żeby łącznie było 7. Moja żona ma M1 Quo jeszcze w starej budzie Aira i też myślę, że w jej przypadku do 8. I to powinien być albo koniec wsparcia macOS-a dla tych układów, albo już taki sensowny rok, po prostu go zostawimy w rodzinie.

[PRZEMEK] No więc właśnie… Tak, to u mnie się dzieje z urządzeniami Apple, że one mają przeważnie 2 albo 3 życia, więc zawsze ktoś tam dostaje w spadku.

[KRZYSZTOF] Ja zawsze mówię, że osoby, które pokupowały M1, jak wchodziły na górce finansowej, bo umówmy się, myśmy te sprzęty kupowali, nawet z tym moim monitorem łącznie, na górkach finansowych i to ogromnych, to i tak nie znamy ani jednej osoby z tego grona, która by narzekała czy coś, a wręcz większość tych osób jest na tyle zadowolona, że tak jak my celuje w jakiś tam horyzont absurdalny, 7-8, czasami nawet więcej lat, nie?

[PRZEMEK] Zgadza się.

[KRZYSZTOF] To był moment w historii. Ciekawe, ciekawe. Chyba szybko drugiego takiego nie będzie miał Apple. **Przechodząc jeszcze płynnie do eventu, który przed nami, to moi drodzy tylko małe przypomnienie, że tuż po Apple Event 9 września, na którym zobaczymy nowe flagowce od Apple i pewnie nie tylko, wspólnie z Mateuszem z kanału Twoja Rzecz, robimy dla Was nasze, naszą rzecz, czyli LIVE'a kolejnego. Będzie to zapewne coś około godziny 21:00 na kanale YouTube Twoja Rzecz.** Szczegóły oraz bezpośredni link do tego wideo, które już możecie sobie zapisać na przykład w liście na później w waszych kontach youtubowych, znajdziecie w opisie tego odcinka. Tam także link do zaproszenia wystawionego jakby inaczej mogło być, w ramach aplikacji Zaproszenia od Apple.

Do zobaczenia i do usłyszenia zatem w przyszły wtorek, a my przechodzimy do głównego tematu tego odcinka.

Co słychać u Synology Przemek? Pytałem co słychać u Ciebie jako fana Apple, to pytam, co słychać u Ciebie jako miłośnika również Synology, no i przede wszystkim w Waszej firmie. Co ciekawego?

[PRZEMEK] No u nas się bardzo dużo dzieje. Mieliśmy... Taki pierwszą próbę wystąpienia na Computex, aktywnie. Mieliśmy bardzo duże stoisko na Computex i odwiedziło nas naprawdę mnóstwo osób. Polecam relację na naszym kanale YouTube, tym globalnym. I to przyniosło nam bardzo dużo informacji i feedbacku od użytkowników, którzy przychodzili i mówili, że właśnie to im się podoba, to im się nie podoba, to by chcieli zobaczyć. Więc cały zespół ten nasz tajwański miał mnóstwo pracy, żeby to wszystko pozbierać i myślę, że z tego bardzo dużo fajnych rzeczy się urodzi w przyszłości.

[KRZYSZTOF] Jak się zbiera taki feedback na żywo w trakcie takiego tworu, takiej tkanki, jakim jest ogromna konferencja, event, nie? W sensie, gdzieś to sobie zapisujecie, segregujecie, tak?

[PRZEMEK] Tak, tak, tam przy każdym stoisku było kilka, czasem kilkanaście osób z tego działu, który jest konkretnie odpowiedzialny za daną część naszych... produktów i oni mieli zadanie zbierać te wszystkie informacje i w jakiś sposób przetwarzać i takie podsumowanie wysyłać do osoby odpowiedzialnej. Odwiedziło nas kilkanaście, kilkadziesiąt tysięcy osób w ciągu tych kilku dni. Więc tak, szaleństwo, jak widziałem na kamerach ile się tych ludzi, bo oczywiście całe nasze stoisko było monitorowane naszym Surveillance, z tymi kamerami 360 nowymi i tymi, które tam mogą liczyć ludzi, więc wszystko było w jakiś sposób ustawione, żebyśmy mieli statystyki i żebyśmy też wiedzieli, czy nam ten cały event się zwraca i myślę, że to się jeszcze w przyszłym roku powtórzy. Feedback jest bardzo pozytywny, a mieliśmy bardzo dużo rzeczy nowych do przekazania, bo wchodzimy na taki nowy rynek, primary storage i to wymagało, żeby się akurat...

[KRZYSZTOF] Powiesz coś więcej, co to za rynek, prostym językiem?

[PRZEMEK] Tak, tak, generalnie jakbyś spojrzał na nasze portfolio, to oczywiście my mamy urządzenie od jednodyskowych po takie, które można, nie wiem, wsadzić 60 dysków w jedną obudowę i to są urządzenia postrzegające na rynku jako od low end po taki SMB, trochę wyższy, podstawowy enterprise, tak? I generalnie tak Synology jest postrzegane, natomiast to nie jest najczęściej krytyczny sprzęt, który jest używany jako ten podstawowy w bardzo dużych organizacjach albo dużych firmach. Tam przeważnie są jakieś takie duże marki, typu właśnie IBM, NetApp czy inni, bo oni mają sprzęt powiedzmy zupełnie innej ligi, czyli taki właśnie do zadań krytycznych, który no nie może być żadnych kompromisów, który też kosztuje dużo, dużo więcej. I my w tej kategorii mieliśmy tak naprawdę takie małe zaczątki sprzętu, typu naszą najwyższe modele serii FlashStation, typu nasz model HD6500, który to można rozszerzyć do 300 napędów. Natomiast to dalej nie wystarczało każdemu pod względem wydajnościowym, czy skalowalności tego sprzętu. I tutaj wchodzi nasz, nasza taka nowa seria PAS, czyli Primary Storage. Ona jest oparta o inną architekturę, o dyski NVMe U3, o dużo, dużo szybsze sieciowe i i protokoły komunikacyjne wewnątrz i zewnątrz, więc to jest tak jakby o powiedzmy trzy, czterokrotnie szybszy sprzęt niż nasz nasz najwyższy, najlepiej, najbardziej wydajny obecnie.

[KRZYSZTOF] Okej, a powiedz mi, na tej konferencji, jak ty oceniasz, w sensie? On oczywiście też wiadomo, że kilkudziesięciu tysięcy się nie da ocenić tak kurwa miarodajnie. Natomiast mieliście już taki *dogfooding* typowy robiony, nie mówisz, że używacie swoich kamer i rozwiązań, więc też sobie sprawdzaliście przy okazji, jak wasze rzeczy działają i co wam mogą dać na tej warstwie danych, co akurat w tych czasach jest znamienne. Natomiast wracając... I jak ty oceniasz w kontekście tego

kogoś, kto przychodził na to wasze stoisko, czy to byli power userzy, czy to byli bardziej ludzie fani, nerdzi, geecy, technologiczni, czy to już byli ludzie z firm, z tego najwyższego szczebla, którzy po prostu szukają konkretnego rozwiązania, czy ten rozkład był jakoś w miarę równy w tych wszystkich grupach?

[PRZEMEK] Przyznam się, nie mam takich statystyk, mogę jedynie powiedzieć z mojego punktu widzenia, bo ja tam spędziłem trzy dni na tym stoisku. Tak, ja byłem akurat na miejscu, mam takie wrażenia bezpośrednio stamtąd, więc to był bardzo duży przekrój ludzi. To byli rzeczywiście użytkownicy biznesowi, bo chyba taka jest forma. Ja też byłem tylko na tych dniach tak naprawdę biznesowych, więc ciężko mi powiedzieć, jak było w ten ostatni chyba dzień. On jest dostępny publicznie dla każdego. Więc tam pewnie było dużo, dużo więcej takich end userów. Ale w tych biznesowych to byli albo to były media, albo to były firmy, które sprzedają nasz sprzęt, albo dystrybucyjne. Albo to były rzeczywiście firmy, które potrzebują jakiegoś tam rozwiązania i chcą porozmawiać, podjąć współpracę itd. Więc z ciekawych osób był Robert Andrews. Na pewno nie trzeba go fanom NAS-ów przedstawiać, bardzo sympatyczny człowiek! Też miałem okazję go poznać i też bardzo duży feedback dla nas przyniósł i był mega szczery wobec nas, wobec naszych też tam menadżerów, więc myślę, że z tego też będzie jakiś jakiś taki pozytywny przekaz.

[KRZYSZTOF] Super, super, to bardzo fajnie i takie wydarzenia są potrzebne, dlatego też wy organizujecie również wydarzenie, które co prawda skupia się na konkretnej dziedzinie, którą chcemy dzisiaj podjąć, czyli bezpieczeństwie, no ale jest też waszym autorskim wydarzeniem, tak?

Więc pytanie, kiedy następna edycja, gdzie? Bo to już za chwilę, no i przechodząc płynnie do tego cywilizacji, bezpieczeństwa w temacie, wydawać by się mogło, w którym jedni powiedzą „Ale to po co o tym gadać, przecież całe NAS-y są jakby z definicji i mają być bezpieczne, to w końcu kopia zapasowa!”, a z drugiej strony to jest taki temat, który myślę, że warto podjąć. Właśnie po to, aby zobaczyć, ile różnych procesów składowych i produktów też wchodzących w coś, co my później końcowi użytkownicy nazywamy po prostu DiskStation czy tam NAS albo po prostu dyskiem na kopię zapasową – musi zagrać, musi się złożyć w jedną spójną całość, żeby faktycznie, no coś mogło być tak oczywiste, że te dane są bezpieczne, nie?

Jak to się wśród zielonych, że tak się kolokwialnie wyrażę, utarło mówić. Jakie to jest wydarzenie i co nam... za horyzoncie się pojawia, Przemek?

[PRZEMEK] Tak. My staramy się co roku robić takie jedno duże wydarzenie w Polsce. Ono też najczęściej jest w kilku krajach w podobnej formie. Akurat

w Polsce my wybraliśmy sobie delikatnie inną formę niż w innych krajach. Więc Polska, Czechy mamy – Security Solutions Day. I te, ta pierwsza część, *security*, jest bardzo istotna, bo jest to wydarzenie organizowane przez Synology, natomiast skupia się na bardzo szeroko pojętym bezpieczeństwie, Więc to nie jest tak,
że klient przychodzi czy tam przychodzi do nas osoba na to wydarzenie i są tylko produkty Synology i mówimy o tych tylko produktach, tylko mówimy o bardzo ogólnym podejściu do bezpieczeństwa. Bo uważamy, że jako lider
w zabezpieczeniu danych powinniśmy też edukować klientów i innych w tej kwestii, bo dla nas jest to inwestycja. Gdyż jak później przejdziemy przez te wszystkie detale, jak ten produkt jest tworzony, to ten użytkownik jest najczęściej tym najsłabszym ogniwem. Więc cała nasza praca, ta inwestycja w to urządzenie, wszystko to co wkładamy, jeżeli nie będziemy mieli świadomego użytkownika, idzie na nic. Więc po to jest ten event, żeby uświadomić klientom i firmom, czy tam organizacjom, że bezpieczeństwo to nie jest tylko, nie wiem, włączenie jakiejś tam funkcji w systemie i na tym się to kończy, tylko jest to cały proces, włącznie z tą jedną jednostką, którą jest człowiek, który musi być zaprojektowany świadomie
i musi mieć ręce i nogi. To wszystko musi ze sobą działać. Więc...

[KRZYSZTOF] Najbliższe tego typu wydarzenie, czyli Security Solution Day 2025, odbędzie się…?

[PRZEMEK] 24 września w Warszawie, w Fabryce Norblina. Zapraszam wszystkich serdecznie, jest to wydarzenie dostępne dla każdego. Wydaje mi się, że są jeszcze miejsca i można taki bezpłatny bilet sobie zarezerwować, zarówno jak się jest firmą, klientem końcowym biznesowym, czy klientem końcowym po prostu. Więc myślę, że link będzie w opisie.

[KRZYSZTOF] Tak, no przede wszystkim tam możecie mieć dostęp nie tylko do Przemka i całej jakby tych ważnych osób z załogi Synology, ale również też do właśnie takich dedykowanych pokazów cyberataków, które wiem, że chcecie przebrać.

[PRZEMEK] Dwie ważne marki, tak? Niebezpiecznik, czyli którego nikomu nie trzeba przedstawiać, więc myślę, że jak ktoś był raz na wykładzie Niebezpiecznika, to wie o co chodzi i jak ja widzę gdzieś, że jest to jest wykład Niebezpiecznika, zawsze jak mogę, to się zapisuję. I drugi, Sun Capital, to jest też nasz partner, który jest firmą promującą bezpieczeństwo z wykorzystaniem technologii VR. Czyli mamy wirtualną rzeczywistość i oni w ten sposób... i w ten sposób starają się pokazać klientowi
z punktu jak on był w środku tego ataku, jak on może reagować, jak to wygląda,

jak trzeba działać, jakie kroki podejmować. To jest dla mnie, moim zdaniem, będzie też ciekawe doświadczenie.

[KRZYSZTOF] Więc zachęcam, nawet jeżeli nie jesteście ze stolicy, żeby się wybrać, a się tym interesujecie na przykład, żeby się wybrać na to wydarzenie, bo jest to raz w roku organizowane faktycznie, a no formuła jest spójna, także od siebie również gorąco, gorąco polecam. Link w opisie do rejestracji, o której wspomniał Przemek.

Przemek, więc jakby bierze się i nasuwa na myśl takie pytanie, jak Synology postrzega bezpieczeństwo, więc je teraz zadaję, natomiast z takim małym przecinkiem, bo wspomniałeś o tym czynniku ludzkim i tak sobie myślę, że to może być dobry punkt wyjścia do całej tej rozmowy, dlatego że w dobie galopującej rewolucji AI, o której mówi się bardzo dużo i ty nawet w naszym ostatnim nagraniu, nie wiem ile to mogło być, z rok temu (?), jakoś tak, wspominałeś, że Synology już wtedy powoli wdraża te rozwiązania AI u siebie, w usługach. Pewnie to się tylko pogłębiło, więc trochę nam jeszcze pewnie zdradzisz za chwilę. No i myśląc sobie o AI, tym bardziej myślę sobie to, o czym wspomniałeś, że dobre cyberbezpieczeństwo to jest przede wszystkim ten fundament ludzki, który jest świadomy tego, z czym on ma styczność. Klikamy tylko, nawet na urządzeniach Apple'a, nie, dalej, dalej, dalej, dalej, no to my sobie to wszystko włączymy. Tylko gdy przyjdzie ta potrzeba, albo przyjdzie ten atak, albo przyjdzie chwila, kiedy musimy sięgnąć do kopii zapasowej, to nic nam z tego, że my coś tam włączymy, bo po prostu przeklikaliśmy się, a ktoś, kto projektował system, zadbał o to, żeby to było trochę w cudzysłowie "idiotoodporne". Jak my nie będziemy wiedzieli, gdzie tej kopii szukać albo co właściwie mieliśmy zabezpieczone, a czego może nie mieliśmy zabezpieczonego, nie? I tu znowu wracamy do tego człowieka, więc wyjdźmy od niego, bo no to jest faktycznie fundament, nie?

[PRZEMEK] Tak, no tak zawsze mówię, że najsłabszym ogniwem całego układu jest właśnie ten element – człowiek, więc możesz mieć super zabezpieczenia, wszystko świetnie zrobione, najnowszą technologię, natomiast jeżeli będziesz miał jeden element, który zawiedzie, to cały ten łańcuch po prostu się przerywa, więc człowiek tutaj jest bardzo istotny. Dlatego jego edukacja, jego świadomość, że coś takiego może być, jest bardzo istotne. Jeżeli chodzi o AI, to to jeszcze bardziej komplikuje sprawy, bo narzędzia, które są w internecie są super jako narzędzia, natomiast tam też na tę chwilę nie ma zdefiniowanych takich granic bezpieczeństwa i granic, które informacje powinniśmy udostępniać, jak bardzo powinniśmy się angażować w te AI i moim zdaniem to też jest kolejne zagrożenie, które tylko będzie się pogłębiać, dopóki nie zostaną ustalone jakieś ramy dla użytkowników i dla firm, których powinni się wszyscy poruszać. Synology podchodzi do tego z dosyć takim dużym

dystansem. U nas bezpieczeństwo danych i prywatność jest takim kluczowym elementem już od podstaw projektowania naszych rozwiązań. Dlatego to, w jaki sposób my zintegrowaliśmy ten AI, też jest zrobione w taki sposób, żeby to było dobre narzędzie, natomiast żeby ono nie było dziurą w całym tym systemie bezpieczeństwa i w ten sposób tak w tym miesiącu była premiera Synology Office AI oraz Mailplus razem z Synology AI Console. Taki zestaw narzędzi, czyli dwie aplikacje dla użytkownika, nasz Office i klient pocztowy i serwer pocztowy, plus konsola, która pozwala podpiąć modele właśnie językowe AI do tych dwóch usług. Przez tę konsolę to jest wszystko filtrowane i tam jest mnóstwo narzędzi, które pozwalają na przykład na anonimizację tych danych, na filtrowanie, na wyłapywanie prywatnych danych, żeby one nie wychodziły poza organizację i tak dalej, więc tak to jest zrobione. Ja polecam przetestować sobie, jak ktoś ma nasze, nasze serwery, to Office jest za darmo. Mailplus jest za darmo z pięcioma kontami, więc można to sobie sprawdzić i przetestować.

[KRZYSZTOF] A jeszcze od razu dopytam, bo pewnie na warstwie testów tego wdrożenia, o którym teraz wspomniałeś, tych pierwszych produktów waszych AI, wyobrażam sobie, że to było dużo większe wyzwanie niż do tej pory. Czy na przykład wy zwiększaliście jakieś grono testerów, mam na myśli testerów manualnych, nie testy automatyczne, czy na przykład to było wyzwanie też w kontekście kadry u was, czy to w Tajwanie, czy w Polsce, nie wiem gdzie jest ten team, który testuje, bo to mnie zawsze ciekawi, jakby tam różne firmy...

[PRZEMEK] Tak, generalnie u nas mamy 3 takie etapy, jak mógłbym powiedzieć. Jest testowanie właśnie automatyczne, przez jakieś tam mechanizmy. Później jest testowanie na ludziach, jak to mówię i najpierw na małych teamach, później my jako team Synology jesteśmy tym testerem. Bo zanim wypuścimy jakiś produkt publicznie, my sami musimy być przekonani, że to działa i że to ma rzeczywiście sens. Więc my byliśmy tym pierwszym testerem. Później były publiczne testy beta, akurat tych aplikacji i konsoli. I dopiero teraz jest release taki publiczny, gdzie wszystko działa. wszyscy mają do tego dostęp.

[KRZYSZTOF] Okej, i ten feedback też do was spływa od tych użytkowników, którzy są z wami wiele lat zapewne, nie?

[PRZEMEK] Tak, tak, tak.

[KRZYSZTOF] No okej, super.

[PRZEMEK] Mamy całe community też i stamtąd też jest bardzo dużo informacji.

[KRZYSZTOF] Jakie są, Przemek, myślę, że można użyć takiego ciężkiego słowa “pryncypia" – takie odpowiedzialne za cyberbezpieczeństwo, no bo jakimi zasadami musicie się jako Synology co do zasady kierować? Bez względu na to, czy mówimy o AI czy czegokolwiek innego dotykamy, to pewnie są jakieś wasze wartości, wasze pryncypia, które zawsze się przykłada do testowania czy projektowania jakiegoś rozwiązania w kontekście jego bezpieczeństwa w całym ekosystemie czy ekosystemie. No bo myślę, że fajnie od tego wyjść. Zanim jeszcze zrzucimy winę, czy będziemy mówili w kierunku ustawodawców, żeby coś zrobili, jakieś prawo ujednolicili, bo to AI jest takie dziwne, no to sami pewnie też macie już od dawna taki wzór.

[PRZEMEK] Tak, ale wzór jest bardzo prosty. I cel jest bardzo prosty, kiedyś zapytaliśmy naszego przełożonego i jednego z naszych szefów, po co i dlaczego my robimy akurat taki krok w naszym rozwoju i w rozwoju naszej firmy i w rozwoju naszych produktów. Odpowiedź była może banalna dla niektórych, bo to było „Bo po prostu chcemy mieć najlepszy na świecie produkt”, w sensie, najlepszy na świecie NAS, który będzie bezpieczny i który będzie dostępny dla każdego.

Wydawałoby się, że to można zrobić dużo łatwiej, dużo taniej, natomiast takie podejście generuje mnóstwo problemów i kompromisów, na które trzeba pójść, bo projektując produkt na lata, nie na rok, na dwa, bo nasz sprzęt jest najczęściej używany, nie wiem, z 8, z 10 lat. Często jest tak, że nawet dłużej. W taki sposób, żeby po pierwsze przez te ileś tam lat móc wspierać ten produkt na najwyższym poziomie, czyli od pierwszego projektu musi być cały, cały łańcuch dostaw. Zarówno części, czy elementy oprogramowania, bibliotek i wszystko musi być przemyślane i też weryfikowane na każdym etapie rozwoju tego.

Więc nie wiem, dla niektórych wydaje się, że zrobienie serwera NAS jest bardzo proste, bo w zasadzie, jakby popatrzeć na obecne rozwiązania na rynku w internecie, jest to bardzo proste, bo można sobie kupić sprzęt, można sobie zainstalować soft, ściągnąć go z internetu i mamy serwer nasz. Natomiast, żeby to było tak jak my chcemy, czyli żeby to było bezpieczne i długotrwałe, to jest to trochę bardziej skomplikowane. Więc tutaj są procedury dotyczące każdego elementu tego sprzętu i je można bardzo łatwo sprawdzić, bo mamy taką fajną zakładkę na stronie, która się nazywa „Bezpieczeństwo” i tam jest opisane wszystko dokładnie, czyli jak wygląda proces planowania i projektowania aplikacji, bo my jesteśmy firmą software’ową. Jakby ktoś nas postrzegał inaczej, my zawsze mówimy, że jesteśmy firmą software'ową, bo to jest główny element i główny produkt Synology.

[KRZYSZTOF] Jak później jest nadzorowany ten cały rozwój, czyli dostaw każdego elementu oprogramowania? Jak jest nadzorowane bezpieczeństwo, czyli cały team, który jest odpowiedzialny za wykrywanie luk w aplikacjach oraz za reakcję, bo ja nie wiem, myślę że to może być dobre pytanie.

[PRZEMEK] Tak, to jest takie pytanie bardzo elastyczne, bo to, że będzie jakaś luka w aplikacji jest 100% pewne. Jesteśmy już na takim etapie rozwoju aplikacji, że one są tak skomplikowane, że nie da się uniknąć luk bezpieczeństwa. To nawet korporacje największe na świecie, typu właśnie Apple czy czy inne, zawsze mają luki bezpieczeństwa, a wydają na to mnóstwo pieniędzy, tak? Więc pytanie, kiedy to się pojawi, jak to jest niebezpieczne dla użytkownika i jak szybko trzeba na to zareagować. W momencie kiedy my mamy tak zwane zero day exploit, czyli jest luka, która jest bardzo istotna i która pozwala na atak na urządzenie zdalne na przykład, który może spowodować dużą szkodę dla niego. Tutaj mamy na to, na analizę tej podatności około 8 godzin i ona powinna być rozwiązana w ciągu 15 godzin. To jest takie założenie, które, standard, który myśmy sobie przyjęli i bardzo łatwo jest to zweryfikować w naszym biuletynie bezpieczeństwa. Wystarczy sobie kliknąć. Tam jest lista podatności, którą my jako członek CVE, Authority i innych organizacji musimy zgłaszać i musimy publikować i jest też czas reakcji, czy ta podatność jest rozwiązana, czy nie jest rozwiązana i jest cały changelog, czyli kiedy była publikacja, kiedy było rozwiązanie.

[KRZYSZTOF] Czy to wymaga po waszej stronie trzymania, że tak powiem – w gotowości – osoby albo grupy osób, która, no nie wiem, a jak na przykład w niedzielę w pół do trzeciej w nocy ktoś wykryje i wam zgłosi, że macie tutaj jakby problem z taką dziurą w waszych systemach, ja wam tu udowodnię, bo proszę bardzo, już to zrobiłem, że się da włamać, to faktycznie podrywacie się i łatacie, no bo jak się rozwiązuje taki problem, Przemek? W sensie, czy to, to jest zawsze, rozwiązaniem jest zawsze aktualizacja OTA, czy to jest po prostu czasami takie załatanie, którego końcowy użytkownik nie widzi, na przykład w postaci nowego update'u bezpieczeństwa i nawet nie musi o nim wiedzieć.

[PRZEMEK] O każdej luce musimy poinformować końcowego. Jesteśmy tutaj zawsze transparentni i nie ma tak, że gdzieś coś ukrywamy i użytkownik nawet nie wiedział, że była dziura. Musimy to zrobić, bo my też popełniamy błędy. Co z tego, że nam się będzie wydawać, że to załataliśmy. Jak ktoś inny sprawdzi to i uzna, że okej, ta łata poszła, natomiast nie załatała wszystkiego albo zepsuła coś innego, bo tak czasami się też zdarza, więc tutaj jesteśmy transparentni, natomiast cały czas jest zespół odpowiedzialny, ten nasz PSIRT. To jest Product Security Incident Response Team. Oni działają non-stop, w sensie mają dyżury i 24 godziny na dobę

ktoś tam jest i jest w stanie przyjąć zgłoszenie i zareagować. Więc to w większości dużych organizacji tak działa, że jest taki zespół, który musi reagować, jeżeli takie ulgi się pojawiają.

[KRZYSZTOF] Co ciekawe, jestem tak swoją drogą, jak duża skala takiego zespołu jest na przykład w takim Apple. Już nie chcę wspominać, albo zróbmy to, wspomnijmy, że była kiedyś taka aktualizacja, co w iPhone'ie chyba 4 albo 4s zepsuła ludziom aplikację telefon i się nie dało jej używać. To pamiętna aktualizacja, ale to wtedy chyba też w ciągu 10 godzin wydali poprawkę, no ale wyobrażam sobie, że tam to musi być, no nie wiem, czy nie w setkach osób liczone.

[PRZEMEK] Na pewno, na pewno, ale to też jest tak, że oprócz tych zespołów, które są wewnątrz organizacji, bardzo często to jest, jak my na przykład, czy Apple, jesteśmy też członkiem większej organizacji.

My jesteśmy członkiem takiej organizacji FIRST. Między innymi Apple i IBM też są członkiem tej organizacji. I duża ilość tych podatności nie wynika z samego kodu napisanego przez Apple, czy przez Synology, tylko właśnie wynika z łańcucha dostaw i z elementów, które są współdzielone, bo w obecnych czasach jest to jasne, że nikt nie tworzy wszystkiego od początku, tylko korzystamy z rozwiązań, które są dostępne, open source jest na tyle rozpowszechnione, że wszyscy z tego korzystamy, natomiast to w jaki sposób kontrolują ten łańcuch dostaw, czy po prostu biorą co jest, czy zanim to jest zostanie zaimplementowane, to weryfikują, to już jest inna kwestia i to jest kwestia polityki firmy, więc jeżeli się coś takiego pojawi. Jakaś biblioteka ma błąd, no to wszyscy członkowie, członkowie tej organizacji dostają natychmiast informację, że jest taki błąd w takiej i takiej bibliotece i każdy team od razu sprawdza, jakie produkty mogą być na to podatne. Jeżeli ten łańcuch dostaw jest monitorowany, to w przypadku naszym, my w ciągu paru sekund mamy listę pakietów i urządzeń, które są podatne, są podatne i które trzeba załatać.
W momencie kiedy firma tego nie ma w ten sposób zorganizowanego, to po prostu wychodzi w praktyce.

[KRZYSZTOF] I tutaj warto dopowiedzieć, bo też rozmawiałem, miałem odcinek z firmą HP realizowany, i tam też w kontekście cyberbezpieczeństwa, ale u nich na maszynach, tak żeby wjechać trochę z kontrastem dla tego słynnego zdania, że Apple jest tutaj najbezpieczniejsze, bo ma Secure Enclave, a nie, okazuje się, że HP też ma coś podobnego i tak dalej, i tak dalej. Natomiast tam padło takie fajne zdanie, parafrazując je oczywiście teraz, że łańcuch dostaw i to, kto dotyka nawet fizycznie opakowania z twoim laptopem, zanim ono trafi do ciebie w twoje ręce i ci je przeniesie kurier, to też jest kwestia zagrożeń bezpieczeństwa, która jest

monitorowana i jest trackowana. I może być tak, że ktoś tego komputera nawet nie odpakował, a i tak on przyjedzie do ciebie na przykład z wgranym, złośliwym oprogramowaniem. Takie rzeczy się już mogą dziać w różnych firmach, się dzieją, są monitorowane i no to są ciekawe wątki, dlatego, że Kowalski o tym no nigdy w ten sposób nie pomyśli. A, wracając do naszego ukochanego Apple, oni również już opracowali system, który na przykład w ich oficjalnych sklepach na całym świecie w tym momencie już aktualizuje iPhone'y bez otwierania pudełek, nie? W sensie, jest taka maszyna, taka szafa i ona to robi po prostu, żeby no klient miał zawsze najnowszy system wgrany. Mimo tego, że z fabryki przyjedzie z tam dwie wersje wcześniejsze i teraz przy premierze zaraz we wrześniu będziemy pewnie te sytuacje tak samo obserwowali, w sensie no my ich nie obserwujemy, ale no tak będzie się działo w tych Apple Store'ach na całym świecie. To jest niesamowite jak się w ten sposób o tym pomyśli.

[PRZEMEK] Zgadza się.

[KRZYSZTOF] I to powiedz mi jeszcze, bo mówiliśmy, co się stanie, gdy się właśnie wydarzy jakiś incydent, a co się dzieje zanim on się wydarzy? To może tak odwrócę pytanie, bo wiem, że wy też stosujecie, wynagradzacie tych, którzy wam odkryją jakieś podatności czy luki w waszych systemach, czy w ogóle w całym ekosystemie? Jak to działa? Co to za program?

[PRZEMEK] Tak, to jest taka forma działalności, która jest bardzo powszechna, jeżeli chodzi o duże organizacje i duże firmy. My też staramy się w miarę naszych możliwości w ten sposób działać. Czyli po pierwsze, współpracujemy z ponad dwustoma takimi researcherami czy tam organizacjami, które zajmują się bezpieczeństwem i oni pierwsi dostają te aplikacje do testowania i mają też możliwość wygrania nagrody w momencie, kiedy, to jest taki bug bounty program, który jest dostępny też na naszej stronie i każdy może tam zgłosić ustawienie czy lukę w bezpieczeństwie, z nagrodami od 5 tysięcy chyba dolarów do 30 tysięcy, jeżeli to jest luka dotycząca naszego systemu operacyjnego. Więc w ten sposób też dużą rzeszę tych użytkowników, czy nawet takich pasjonatów, którzy lubią nasz sprzęt, a są specjalistami od bezpieczeństwa, zachęcamy do tego, żeby oni najpierw nam przekazali taką informację z jakimś tam czasem na reakcję, bo taka jest generalnie zasada. Jeżeli haker, czyli ten dobry haker, znajdzie jakąś lukę, to z zasady powinien najpierw powiadomić odpowiedzialną firmę za to, w momencie kiedy ona nie zareaguje w ciągu określonego tam czasu, ma prawo to opublikować. Więc to jest jedna rzecz, a druga rzecz, my bardzo często staramy się też uczestniczyć w tych takich konferencjach dla hakerów, gdzie oni po prostu mają konkurs na złamanie zabezpieczeń danego sprzętu i wielu vendorów im udostępnia

jakiś nowy sprzęt, czy nowe oprogramowanie właśnie tylko po to, żeby w pierwszej kolejności dostać informację od nich, co poszło nie tak, zanim to trafi na rynek. Więc tutaj też mieliśmy takich kilka przykładów, przypadków, że to nasze oprogramowanie zostało złamane bardzo szybko i znaleziono kilka takich krytycznych błędów, ale dzięki temu, że my zrobiliśmy to zanim to się pojawiło na rynku, byliśmy w stanie to bardzo szybko załatać.

[KRZYSZTOF] I to też jest na przykład, bo to jest coś na wzór hackathonów, nie? Wy to sobie oczywiście nazywacie bug bounty program w Synology, ale te same wydarzenia to mówmy wprost, są hackathonami dla hakerów po prostu, tak?

[PRZEMEK] Tak, tak.

[KRZYSZTOF] I tak sobie myślę, że kiedy my mówimy o takim małym domowym NAS-ie, to jeszcze pół biedy, nie? Ale jak mówimy o wdrożeniu na przykład, nie wiem, w jakimś szpitalu...

[PRZEMEK] Zgadza się. To jest dobrze wykryć wcześniej, bo ta skala może zrobić różnicę. Tak, a biorąc pod uwagę nasz sprzęt, gdzie 80% naszych urządzeń ma ten sam system, to jest bardzo istotne, żeby każdy miał ten sam poziom bezpieczeństwa. W przypadku tych nowych systemów PAS, oczywiście tam ten soft będzie mocno zmodyfikowany, bo tam nie są potrzebne wszystkie funkcjonalności i bardzo często tak się robi, że jak jest dedykowany, specjalizowany sprzęt, to wycina się wszystko, co jest niepotrzebne, między innymi z powodu bezpieczeństwa, żeby uniknąć błędów, mogą być w tych elementach zbędnych.

[KRZYSZTOF] No tak, na poziomie użytkownika, bo mówiliśmy o tym czynniku ludzkim na początku. Dobrym przykładem jest seria B od was, na przykład BeeStation, tak, czy BeeDrive.

[PRZEMEK] Tak.

[KRZYSZTOF] Ona też jest mocno okrojona na poziomie zwykłego SRM-a, tak?
To nie znaczy, że ona grupie docelowej tych produktów nie dostarcza tego, co było w założeniach z samego początku, bo umówmy się, klient BeeStation to nie jest klient NAS-a, do którego wsadzi 15 dysków i to jest youtuber, to jest zupełnie inny klient.

[PRZEMEK] Tak, tak, no to o to chodzi w tym wszystkim, żeby przede wszystkim produkt był skierowany do tego docelowego klienta i był tak skrojony, żeby jemu najlepiej spełniał jego oczekiwania. To jest podstawa projektowania jakiegoś produktu konsumenckiego, natomiast to też nam pomaga zachować

bezpieczeństwo, bo im mniej elementów jest w danym systemie, tym łatwiej jest nad tym wszystkim zapanować. Jeżeli chodzi o, tak.

[KRZYSZTOF] Jeszcze dopowiem do zobrazowania dla, dla moich słuchaczy.
To trochę jest tak, jak z tym faktem, że iOS powstał na bazie macOS-a, chociaż jest totalnie mniej potrafi niż macOS do dzisiaj, a znowu na bazie iOS'a powstawały kolejne systemy, watchOS, tvOS czy nawet oprogramowanie HomePodów, no i tam siłą rzeczy nie zrobicie tego, co na iPhone'ie i Bogu dzięki swoją drogą!

[PRZEMEK] Tak, tak, no Apple robi dokładnie tak samo, oni biorą jakiś tam core,
z którego tworzą system, natomiast wycinają wszystko, co jest niebezpieczne, niepotrzebne, bo to jest najczęściej takim elementem, który generuje błędy, bo można by zostawić oczywiście te niepotrzebne rzeczy, natomiast jeżeli ich nikt nie będzie przeglądał za każdym razem, przy każdej aktualizacji, to w końcu tam się znajdzie jakieś, jakaś luka. I tutaj może wróćmy do tego użytku...

Użytkownika, bo on jest tutaj tym elementem kluczowym. My staramy się tak projektować aplikacje, aby jak najbardziej pomóc w tym użytkownikowi w sposób nieangażujący. Pomóc mu zachować to bezpieczeństwo właśnie przez taką podwójną autentykację, która nie zawsze wymaga jednorazowych haseł, bo to jest dla większości denerwujące i nie każdy to lubi. Więc to można zastąpić aplikacją,
w sensie powiadomieniem w aplikacji, tak? Czy, czy implementacją tych Apple Passkeys. To też zaczęliśmy robić już w naszych usługach, tak żeby klient nie musiał pamiętać hasła do usługi, gdzie te hasło musi mieć kilkanaście znaków, bo inaczej nie przejdzie. Więc tutaj jeżeli zeskanuje kod telefonem, to ten Passkey ładnie mu przejdzie i się będzie mógł zalogować. Bezpieczeństwo jest bardzo istotne, natomiast ono musi być tak zrealizowane, żeby użytkownik chciał je włączyć, bo oczywiście można zrobić bezpieczny system z hiper wymagającymi hasłami. Użytkownik, jeżeli będzie musiał wykonać tak duży wysiłek, żeby to działało i to, więc cały ten wysiłek pójdzie na marne.

[KRZYSZTOF] Plus, zwłaszcza jeżeli ten wysiłek będzie musiał być podejmowany każdorazowo, no nie?

[PRZEMEK] Zgadza się. To jest fakt.

[KRZYSZTOF] Gdzie szukać w ogóle wiedzy, bo mówisz o niej bardzo dużo
i mówiłeś dzisiaj w naszej rozmowie, to gdzie szukać wiedzy? Wiedzy, dla każdego tak naprawdę, i dla tego Kowalskiego, i dla tego Smitha, który siedzi już na stanowisku administracyjnym, czy administratorskim i zarządza gdzieś tam flotą

urządzeń, czy serwerami. Gdzie szukać tej wiedzy w kontekście waszego ekosystemu najlepiej i obserwować?

[PRZEMEK] To, co ja zawsze wszystkim radzę, to założenie konta Synology. To jest takie konto darmowe, które można sobie założyć na naszej stronie i pozwala ono przede wszystkim zalogować się do naszych usług, ale oferuje też biuletyn bezpieczeństwa i on jest wysłany, jest spersonalizowany, więc jest wysyłany do konkretnych osób z konkretnym tematem.

Jeżeli macie konkretne urządzenie zarejestrowane na koncie, to dostajecie wszystkie informacje o ewentualnych lukach. Jest oczywiście nasz biuletyn bezpieczeństwa też dostępny na stronie, więc jeżeli ktoś chce sobie wejść, po prostu w każdej chwili można wejść. Ja dzisiaj nawet wchodziłem, sprawdziłem, jakaś luka się nawet dzisiaj pojawiła. Więc to jest jeden z elementów, czyli ta konta Synology, tam można też się zapisać na nasze webinary, w sensie na mailingi o webinarach, o wydarzeniach, więc to jest fajna rzecz.

Druga rzecz. Warto korzystać z naszej aplikacji Secure Sign In. To jest taka uniwersalna aplikacja do logowania do naszych systemów, ale też do podwójnej autentykacji i jest o tyle fajna, że ona też może działać jako zamiennik Google Authenticator czy Microsoft Authenticator, bo one są ze sobą zgodne, więc ja mam akurat tylko naszą aplikację i korzystam też z tych innych usług.

I trzecią taką usługą, która też jest w podstawowej wersji darmowa dla każdego użytkownika Synology jest Synology Active Sign-in. To jest taka usługa do monitorowania serwera. I tam ona monitoruje i gromadzi statystyki z urządzenia, potrafi wykryć jakieś zachowania nietypowe. Na przykład jak ja ostatnio byłem na wakacjach i logowałem się gdzieś tam z Chorwacji na urządzenia, to od razu dostałem powiadomienie, że coś jest nie tak. Że to jest miejsce i czas jest nietypowy dla moich zachowań, więc powinienem to zweryfikować, tak?

Więc ta usługa też jest fajna, jak ktoś ma, jest administratorem powiedzmy większej ilości serwerów, tam kilkunastu, kilkudziesięciu, to oczywiście też może sobie dokupić taki pakiet, który będzie mu pozwalał na monitorowanie tych dodatkowych serwerów, włącznie ze statystykami, nie wiem, tam kilka miesięcy wstecz, więc tam są statystyki z użycia dysków, procesora, można sobie to cofnąć do konkretnego momentu w czasie, żeby sprawdzić, co się działo i można też zarządzać serwerami innych użytkowników, które są podpięte pod inne konta. To już taka na usługę, a bardziej zaawansowane, ale też można to wykorzystać.

To są takie podstawowe rzeczy. Polecam też naszą stronę z tą zakładką bezpieczeństwo, jak ktoś chce się zgłębić w detale, jak my rozwijamy oprogramowanie, jakie są nasze takie podstawowe mechanizmy, skąd się te aplikacje biorą i tak dalej. To wszystko jest tam świetnie opisane. Powiem tak, są to standardy najwyższe na świecie, jak powinno to być robione i warto czasem tam zajrzeć i zobaczyć, bo nie każda firma jest tak transparentna i pokazuje jak to jest u nich robione. I nie każda w ogóle korzysta i jest świadoma z tego. Gdybyśmy spojrzeli na rynek NAS-ów, to jest dużo nowych graczy na rynku, którzy robią super sprzęt. I tutaj nie mogę nic złego powiedzieć o tym. Natomiast jeszcze nie są na tym etapie, w którym zauważyli, że ten element jest tak bardzo istotny dla nich, bo do tego podejrzewam dojdą za rok, dwa, kiedy rzeczywiście coś się wydarzy.

[KRZYSZTOF] Ale to też jest inna kwestia, że jakby nowe firmy bez względu na to, jakie by nie robiły produkty i jak designerskie by one nie były, bo umówmy się, człowiek kupuje też wzrokiem, to nie mają waszego bagażu doświadczeń liczonego w latach, nie jak nie w dekadach! Jakby waszego banku widzenia o tym, co może pójść nie tak, i to jest ten główny case, jak ktoś czasami się zastanawia, czy na przykład właśnie wziąć coś, co niekoniecznie jest arcydziełem, jeżeli chodzi o design, ale ma 20 lat jakby backgroundu za sobą, czy wziąć jakąś nową...

[PRZEMEK] Zgadza się. No to, to też, jak mówiłem, cały ten proces, którym my przeszliśmy przez te 25 lat, daje nam doświadczenie i takie trochę inne spojrzenie na całe tę branżę i urządzenie i na użytkownika. Więc czasami użytkownicy nie rozumieją ruchów, które my podejmujemy, bo im się wydaje, że robimy coś wbrew logice, wbrew temu, co oni by chcieli, natomiast tak jak to jest w przypadku Apple czasami, że też nikt nie rozumie, dlaczego oni coś zrobili i że to jest w ogóle sprzeczne z tym, co użytkownicy chcą, ale gdzieś z tyłu jest w tym logika, o której nie zawsze możemy powiedzieć, a która składa się na to, że chcemy zrobić jak najlepszy produkt dla użytkownika.

[KRZYSZTOF] I telefon, jaki ludzie by chcieli, licząc od pierwszego iPhone'a, to prawdopodobnie przypominałby on Frankensteina i posiadał wszystkie do tej pory wymyślone przez ludzkość złącza i był rozmiaru pokoju, więc to takie dobre zakończenie. Jest taki obrazek w sieci zresztą, bo jak go znajdę, to wam podlinkuję w opisie.

Przemek, bardzo ci dziękuję, nie będę Cię ciągnął za językiem, co na roadmapie Synology nas jeszcze czeka, bo wiem, że przyjdzie czas, to chętnie się tym podzielisz. Natomiast na pewno od siebie życzę Ci tego, żebyś to jakoś ogarniał, bo jest tego bardzo dużo i to już wybrzmiało w tym odcinku. Także cierpliwości,

wytrwałości także w kontekście Waszych klientów, ale przede wszystkim Was jako team, bo pewnie czasami, nieraz są takie momenty, że ma się już tego trochę dość, a mimo tego idziecie do przodu i cały czas próbujecie być tym liderem i jesteście nim. Także od siebie na pewno życie tej wytrwałości, ona się nam przyda wszystkim, myślę w nadchodzących czasach.

[PRZEMEK] Tak, tak. Ja dziękuję oczywiście za to. My nasz team oczywiście rozwijamy i zatrudniamy, więc warto sprawdzać też oferty pracy w Synology.

[KRZYSZTOF] Polecamy, pewnie!

[PRZEMEK] Tak, polecamy. Natomiast cały temat bezpieczeństwa myślę, że będzie się pojawiał jeszcze w przestrzeni publicznej bardzo często, dlatego jeszcze raz zapraszam na to nasze wydarzenie, bo myślę, że to... I to pozwoli wszystkim, którzy się tam pojawią, spojrzeć trochę inaczej na to, dlaczego Synology działa tak jak działa i robi takie kroki, jak je robi i że to ma głębszy sens.

[KRZYSZTOF] I przede wszystkim, że za tym stoją konkretni ludzie.
I tak zakończymy. Bardzo dziękuję Przemek.

[PRZEMEK] Dziękuję bardzo. No do usłyszenia.

[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]