CYFROWA POLSKA

Cyberbezpieczeństwo urządzeń końcowych po 2022 roku.

Wyzwania i możliwości. Polska, Europa, Świat.

Warszawa, sierpień 2023 r.

Spis Treści

Wstęp

Ponad 230 milionów maili, 6 milionów zapytań w przeglądarce i 100 tysięcy godzin wirtualnych spotkań – między innymi tyle się dzieje w Internecie w ciągu każdej jednej minuty. Tylko w 2022 roku stworzono, skopiowano i **skonsumowano 97 zettabajtów** (czyli 1024^7 bajtów)[1] **danych, przez 5,16 miliardów użytkowników internetu na całym świecie**.

W Polsce, także w 2022 roku, **88.4%** obywateli aktywnie korzystało z internetu, najczęściej za pośrednictwem smartfona - tak robiło aż **93.6%** osób[2]. Podobnie było w przypadku polskich przedsiębiorstw, w których internet pełnił – i zapewne nadal pełni - bardzo ważną rolę w ich funkcjonowaniu – korzystało z niego aż **91,4%** firm, a dla **36,5%** był narzędziem kluczowym, niezbędnym do prowa--dzenia podstawowej działalności firmy. **70,7%** przedsiębiorców korzystało z dostępu mobilnego w telefonie komórkowym, prawie połowa z dostępu stacjonarnego, a **43,8%** z dostępu mobilnego na komputerze, laptopie czy też innym urządzeniu przenośnym[3].

Ale 2022 rok to nie tylko liczby potwierdzające dynamiczny rozwój technologii cyfrowych. Po okresie pandemii i związanej z nią technologicznej rewolucji w pracy czy edukacji, w której branża cyberbezpieczeństwa odgrywała kluczową rolę, zapewniając odpowiednią cyfrową ochronę, kolejnym wyzwaniem okazały się cyberzagrożenia wynikające z pełnoskalowej agresji Rosji na Ukrainie. Inwazji, która zmieniła wszystkie dotychczasowe priorytety i wektory działania, wykorzystując Internet do niespotykanej dotąd skali cyberagresji. Skalę i problem potwierdzają dane Check Point Research, które jasno wskazują, że **liczba ataków w pierwszych trzech kwartałach 2022 roku w Polsce była o kilkanaście pro-cent wyższa niż rok wcześniej, w trakcie pandemii. Dla całej branży – od firm technologicznych, przez administrację państwową po użytkowników – był to ogromny test sprawdzający wydolność i odporność krajowego systemu cyberbezpieczeństwa.**

Niniejsza publikacja zawiera nie tylko aktualne dane dotyczące obszaru cyberbezpieczeństwa w skali mikro i makro, ale także perspektywy dotyczące wykorzystania sztucznej inteligencji oraz technologii kwantowej na rzecz szeroko rozumianej cyberochrony. Znajdują się w niej także rekomendacje nie tylko dla branży cyfrowej, ale i dla użytkowników urządzeń mobilnych. Bo to one poprzez swoją powszechność stają się celem coraz to bardziej wyrafinowanych i precyzyjnych ataków przeprowadzanych na szeroką skalę.

1. Raport firmy Domo – „Data never sleeps 10.0" – *https://www.domo.com/data-never-sleeps*
2. Raport „DIGITAL 2023: GLOBAL OVERVIEW REPORT" - *https://datareportal.com/reports/digital-2023-global-overview-report*
3. Badanie klientów instytucjonalnych przeprowadzone w 2022 roku realizowane przez Urząd Komunikacji Elektronicznej - *https://www.uke.gov.pl/akt/badanie-klientow-instytucjonalnych-przeprowadzone-w-2022-roku,471.html*

MICHAŁ KANOWNIK

Prezes Związku Cyfrowa Polska

Jeśli polska gospodarka ma w najbliższych latach osiągnąć pozycję cyfrowego challengera, na co wskazuje wiele prognoz, to nie może poddać się w walce konkurencyjnej w zakresie technologii. Zaawansowane technologie, innowacyjność, rozwój sieci 5G, technologie kwantowe, sztuczna inteligencja - to tylko wycinek możliwości dla przyszłości polskiej ekonomii. A z drugiej strony - rozwój kompetencji przyszłości, kadr i specjalistów, podnoszenie świadomości społeczeństwa na temat cyberzagrożeń, czyli wyzwania, które wciąż wymagają pracy, zaangażowania i współpracy na poziomie administracja-biznes.

To wszystko łączy cyberbezpieczeństwo, bo jest ono wyznacznikiem promowania inwestycji państwa i podmiotów prywatnych, a także dojrzałości i odporności na ataki, jakie wymierzane są w polską gospodarkę. Pełnoskalowa inwazja Rosji na Ukrainę uwarunkowała szereg działań takich jak poszerzanie współpracy państwa z branżą cyfrową czy zwiększanie inwestycji w obszarze cyberochrony. Jednak nie może ona ograniczać rozwoju polskiego rynku cyfrowego, zwłaszcza, że w 2030 ma on stanowić 9% prognozowanego PKB. Jak każdy kryzys, także i skrajnie trudna sytuacja za naszą wschodnią granicą stanowi swego rodzaju szansę. Należy ją wykorzystać w celu budowy lepszej ochrony polskich przedsiębiorstw i gospodarki.

1. Zagrożenia cyfrowe

1.1. Świat

Im bardziej społeczeństwo staje się zależne od rozwoju technologii cyfrowych, oraz im powszechniejszy staje się dostęp do Internetu, tym szybciej rozwijają się metody i narzędzia cyberprzestępców. Także tych, którzy służą agresorowi w inwazji na Ukrainie. Według Check Point Research, **w 2022 roku szkody wywołane przez cyberprzestępstwa przekroczyły globalnie wartość 8,44 bilionów dolarów, a w kolejnych latach będą się one zwiększały średnio o 3 biliony dolarów licząc rok do roku.** Z kolei, jak wskazuje firma analityczna CyberSecurity Ventures, gdyby potraktować straty wyrządzone przez cyberprzestępców jako PKB państwa, uzyskalibyśmy wartość równą PKB trzeciej gospodarki świata, po USA i Chinach. Co więcej, cyberprzemoc nie dotyczy już tylko dużych firm, administracji czy instytucji państwowych. Dziś na celowniku może być każda, nawet najmniejsza firma, a także zwykli internauci.

Do najczęściej wykorzystywanych ataków należą:

Ataki DDoS (Distributed Denial of Service)
polegają na przeciążeniu zasobów systemowych, takich jak serwery i sieci, poprzez jednoczesne generowanie ogromnej liczby zapytań lub ruchu, równocześnie z wielu komputerów. Celem takiego ataku jest zablokowanie dostępu do usług lub stron internetowych dla ich użytkowników. Atak na estońskie witryny rządowe, na litewską firmę energetyczną Ignitis Group, na greckiego dystrybutora gazu ziemnego DESFA, na Twittera, ale także na polskie firmy i instytucje - to tylko kilka wybranych sytuacji, jakie miały miejsce w 2022 roku. Według badań przeprowadzonych przez Instytut Ponemon, **średni koszt ataku DDoS w przeliczeniu na minutę przestoju wynosi 22 tys. dolarów, a średni czas przestoju na atak DDoS wynosi 54 minuty.** A to jedynie policzalne koszty – kwoty utracone w związku z utratą własnościintelektualnej, obsługą prawną, koniecznością odzyskiwania danych czy też z procesami produkcyjnymi trudno oszacować w jakiejkolwiek walucie.

Phishing

to technika, w której cyberprzestępcy podszywają się pod firmy energetyczne, kurierskie, operatorów telekomunikacyjnych, dostawców usług płatności mobilnych, ale też instytucje państwowe, i starają się wyłudzić od swojej ofiary pieniądze lub nawet dostęp do konta bankowego. Często wykorzystują fałszywe e-maile, strony internetowe lub komunikaty, aby nakłonić użytkowników do udostępnienia swoich danych. Przestępcy rozsyłają je z informacją opartą na socjotechnice, czyli taką, która ma skłonić ofiarę do określonego działania, na przykład przez kliknięcie w podany w wiadomości link. Pośpiech i nieuwaga sprzyjają cyberoszustom, którzy tylko liczą na to, że w krzątaninie codziennych spraw ofiara nie zwróci uwagi, że właśnie dokonuje zakupów online na fałszywej witrynie, ulega prośbie rzekomego znajomego o pożyczkę, której dokonuje przez szybki przelew, lub też otwiera niebezpieczne, choć na pierwszy rzut oka niewzbudzające podejrzeń załączniki. Z raportu „Cyber Threat Report Q1 2022" wynika, że **w Europie aż o 37 proc. wzrosła liczba ataków phishingowych. W pierwszym kwartale 2022 roku zostały one zablokowane 64 miliony razy w porównaniu z 47 milionami rok wcześniej.**

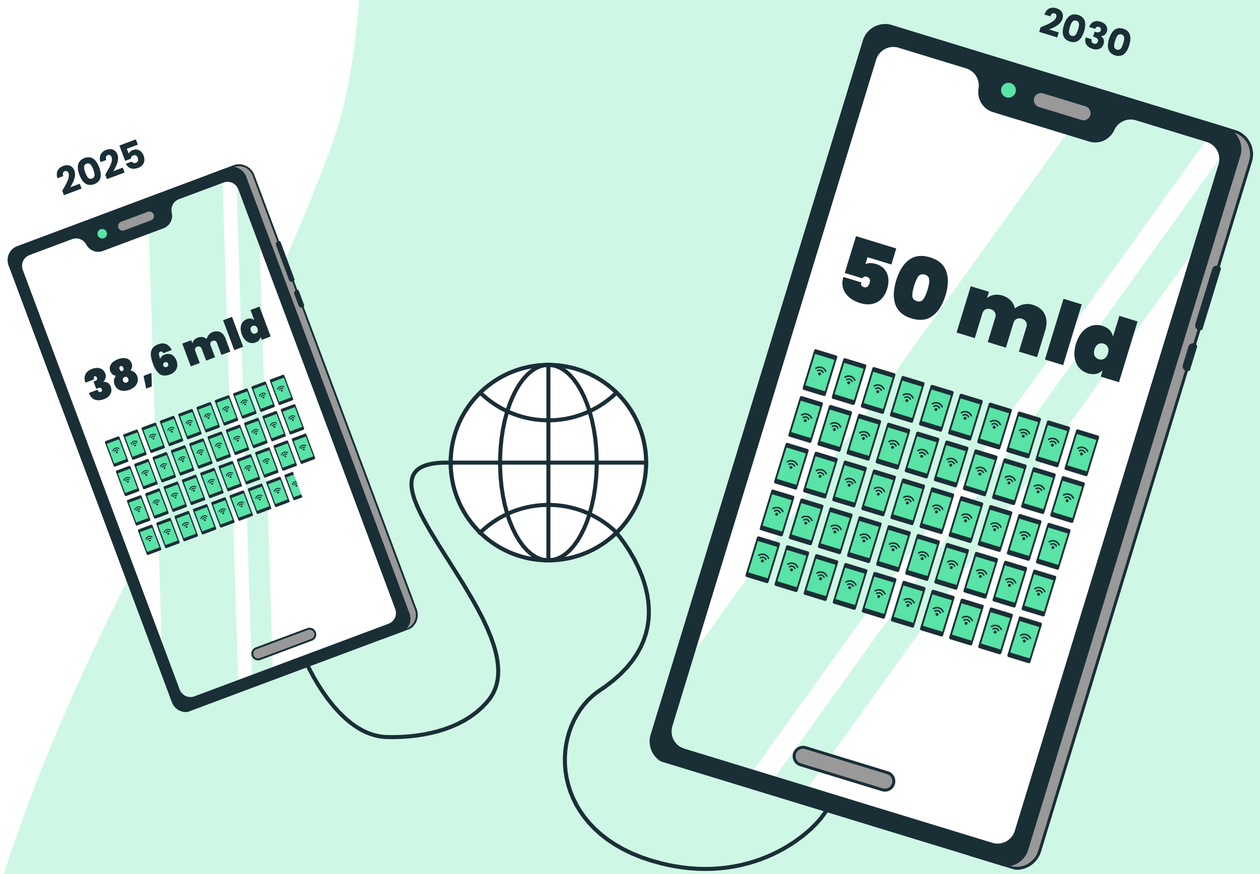
Ransomware

to z kolei złośliwe oprogramowanie, które szyfruje pliki na komputerze ofiary i żąda okupu w zamian za ich odblokowanie. To bardzo opłacalny rodzaj ataku dla cyberprzestępców, którzy mogą zarabiać ogromne sumy pieniędzy na szantażowaniu użytkowników. Według raportu „Talos Incident Response Trends" ataki ransomware oraz działania pre-ransomware stanowiły **aż 40 procent zagrożeń cyberbezpieczeństwa zaobserwowanych w 2022 roku.** Najaktywniejsze były organizacje cyberprzestępcze Vice Society oraz Hive, natomiast najczęstszy obiekt ataków stanowiły usługi finansowe, systemy rządowe oraz energetyka.

Według prognoz ekspertów ENISA - Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, działającej na rzecz osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w Europie, **w najbliższym czasie powinniśmy przygotować się na coraz bardziej zaawansowane i zróżnicowane ataki.** Nie oznacza to jednak, że hakerzy stosować będą tylko nowe techniki – nadal sięgać będą po aktualnie stosowane metody, lecz w nieco zmienionej formie.

Według ENISA 10 najbardziej istotnych cyberzagrożeń, z którymi będziemy mieli do czynienia do 2030 roku, to:

1. Ataki na łańcuchy dostaw z użyciem złośliwego oprogramowania.
2. Zaawansowane kampanie dezinformacyjne.
3. Inwigilacja cyfrowa i utrata prywatności w cyberprzestrzeni.
4. Błędy ludzkie oraz wyeksploatowanie starszych systemów w ekosystemach cyber-fizycznych.
5. Ukierunkowane ataki wzmocnione danymi pochodzącymi z inteligentnych urządzeń.
6. Zagrożenia dla infrastruktury kosmicznej wynikające z braku stosowania odpowiednich zabezpieczeń.
7. Powstanie zaawansowanych zagrożeń hybrydowych łączących świat online i offline.
8. Ataki hakerskie na organizacje, którym brak umiejętności i kompetencji w zakresie cyberbezpieczeństwa.
9. Cyberataki na transgranicznych dostawców usług ICT powodujące niedostępność infrastruktury krytycznej.
10. Nadużywanie sztucznej inteligencji i manipulowanie algorytmami AI.



W **2025** roku na świecie będzie działać **38,6 miliarda** urządzeń podłączonych do sieci internetowej, a w **2030** roku - **50 miliardów**.

4. *Prognozy ENISA - https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030?fbclid=IwAR1u3v8BuJfMKjTdeBOFErBu7OQQDQxH67JsR5El6ne1hheFTsdzmuxiyOI*

1.2. Polska

Jak pokazują dane firmy Check Point Research, **w ciągu ostatnich dwunastu miesięcy hakerzy zwiększyli liczbę ataków na polski sektor użyteczności publicznej o blisko 500% – z 643 (w styczniu 2022 r.) do 3459 tygodniowo! To absolutny rekord.**[5] Z kolei raport „Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu" przygotowany przez firmę KPMG podkreśla, że aż **58%** badanych organizacji odnotowało w 2022 roku incydenty polegające na naruszeniu bezpieczeństwa. Oznacza to, że ubiegły rok mógł być bezpieczniejszy pod względem prób cyberataków w porównaniu do 2021 roku. Optymizm studzi jednak fakt, że w przypadku aż jednej trzeciej badanych firm wzrosła intensywność prób naruszeń bezpieczeństwa. Jest to najwyższy wynik od pięciu lat. Jednocześnie aż **12%** firm przyznało, że zanotowało 30 i więcej incydentów bezpieczeństwa, co świadczy o wzroście aktywności cyberprzestępców. 1/5 ankietowanych organizacji odnotowała w 2022 roku wzmożoną aktywność cyberprzestępców w związku trwającą wojną w Ukrainie. Co ciekawe, **10% badanych firm, które w przeszłości doświadczyło cyberataku przyznało, że jego wystąpienie nie zmieniło niczego w podejściu organizacji do zapewnienia bezpieczeństwa.**[6]

Tymczasem „Badanie klientów instytucjonalnych" przeprowadzone w 2022 roku przez Urząd Komunikacji Elektronicznej pokazało, że nie wszyscy polscy przedsiębiorcy korzystają z rozwiązań zwiększających bezpieczeństwo w sieci. Z oprogramowania antywirusowego korzysta tylko **84,6%** przedsiębiorstw, z managera haseł - **40,2%**, a z dwustopniowego logowania – **35,4%**. Co piąta polska firma korzysta z połączenia VPN, a co czwarta - z szyfrowanych wiadomości i połączeń.[7] Choć te statystyki nie brzmią optymistycznie, to jednak nastąpiła poprawa w korporacyjnym podejściu do cyberbezpieczeństwa w organizacjach. **61%** z nich wpisało w obowiązki pracowników regularny monitoring, a w **36%** powierzono go zewnętrznej firmie. Również 36% firm powołało w swoich strukturach komórkę SOC (Security Operations Center) do monitorowania zagrożeń, ale w większości przypadków nie działa ona całodobowo. W ponad jednej trzeciej firm monitoruje się bezpieczeństwo kontrahentów (**37%**), a **26%** prowadzi tzw. Threat Hunting, poszukując cyberprzestępców, którzy mogą być już w chronionej infrastrukturze. Niestety aż **57%** respondentów przyznało, że logi bezpieczeństwa nie są jednak w ich organizacjach przeglądane regularnie.[8]

---

5. *https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/masowe-ataki-hakerow-na-polska-infrastrukture-35-tys-atakow-tygodniowo/g2t30dx*
6. *„Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu" KPMG, 2022. https://kpmg.com/pl/pl/home/insights/2023/02/barometr-cyberbezpieczenstwa-2023-detekcja-i-reakcja-na-zagrozenia-w-czasie-podwyzszonego-alertu.html*
7. *„Badanie klientów instytucjonalnych przeprowadzone w 2022 roku" Urząd Komunikacji Elektronicznej - https://www.uke.gov.pl/akt/badanie-klientow-instytucjonalnych-przeprowadzone-w-2022-roku,471.html*
8. *„Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu" KPMG, 2022. https://kpmg.com/pl/pl/home/insights/2023/02/barometr-cyberbezpieczenstwa-2023-detekcja-i-reakcja-na-zagrozenia-w-czasie-podwyzszonego-alertu.html*

98% **Polaków używało telefonów komórkowych (w tym 97,6 proc. smartfonów)**

Najsłabszym ogniwem okazują się jednak pracownicy. Według badań firmy Safetica, aż **80%** przedsiębiorstw doświadcza utraty danych w wyniku błędów popełnionych przez pracowników lub ich celowych zachowań. Najczęściej wyciek danych spowodowany jest przez pracowników, którzy przechodzą do pracy do firmy konkurencyjnej lub rozpoczynają własną działalność gospodarczą. Według badań Instytutu Ponemon w głównej mierze wykradane są informacje o klientach **(61%)**, własność intelektualna **(56%)** oraz informacje o konsumentach **(47%)**.

W przypadku ataków typu ransomware – czyli wykradanie lub szyfrowanie danych firm i wymuszania okupu, to ich ofiarą stało się **¾** polskich przedsiębiorstw. Jak pokazują dane firmy Sophos, **22%** z nich poniosło koszt od **2,8 mln** do nawet **5,8 mln zł.** Co dziesiąte przedsiębiorstwo zanotowało straty operacyjne rzędu od **5,8** do nawet **29 mln zł.** Aż **62%**. przyznało, że ransomware miał poważne skutki dla działania biznesu, a jedynie **5%** firm nie odczuło negatywnego wpływu ataku na codzienną działalność. **Co ważne, połowa rodzimych przedsiębiorstw, których dotknął ten problem, zapłaciła przestępcom. Średnia wartość okupu w Polsce to 670 tys. zł.**

Jednak nie tylko polscy przedsiębiorcy byli i są narażeni na działania cyberprzestępców – szczególnie, że wpływ na nie miała toczona za naszą wschodnią granicą wojna. Najczęściej atakowany był sektor badań i edukacji, a na drugim miejscu był sektor rządowy, w tym szczególnie infrastruktura krytyczna, która jest kluczowa dla ciągłości funkcjonowania państwa.

W marcu i kwietniu 2022 roku grupa Killnet, w skład której wchodzą inne nieustrukturyzowane grupy hakerów sympatyzujące z Rosją, przeprowadziła atak DDoS na witrynę internetową polskiego Sądu Najwyższego. Ofiarami ataków grupy padły również strony internetowe ośmiu polskich lotnisk, NBP, Grupy Azoty i innych podmiotów rządowych, a także firm prywatnych (m.in. Castorama, Orange i mBank).

9. *Cyberataki spod znaku wojny – https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/ataki-hakerskie-w-2022-lista*

Jak wskazuje Raport Orange CERT, zaledwie w kilkadziesiąt godzin od agresji Rosji na Ukrainę przestępcy przygotowali i dystrybuowali kampanie, których tematami były fałszywe zbiórki pieniędzy pod pretekstem pomocy armii ukraińskiej lub uchodźcom. Głównym kanałem dystrybucji fałszywych linków były serwisy społecznościowe, gdzie wykorzystywane były przejęte konta i na zasadzie „kuli śnieżnej" dystrybuowane dalej przez nieświadomych zagrożenia użytkowników. Podobnie jak w przypadku innych tego typu kampanii, te miały na celu przejęcie dostępu do kont społecznościowych oraz do bankowości elektronicznej i wykradzenie lub wyłudzenie środków pieniężnych wysyłanych później na konta „słupów" lub portfele kryptowalutowe .

Według specjalistów CERT Polska – zespołu działającego w strukturach Państwowego Instytutu Badawczego NASK, na bieżąco monitorującego i reagującego na to, co dzieje się w polskim internecie, dzięki licznym kampaniom edukacyjnym, informacjom prasowym i ostrzeżeniom publikowanym w mediach społecznościowych, w polskim społeczeństwie znacznie wzrosła wiedza o cyberzagrożeniach. Przełożyło się to na rekordową liczbę zgłoszeń. **W 2022 r. do CERT Polska wpłynęło ponad 322 tys. zgłoszeń, co skutkowało obsłużeniem 39 tys. incydentów. To ponad 34% wzrost zarejestrowanych incydentów w zestawieniu z 2021 r., zaś liczba wszystkich zgłoszeń wzrosła o blisko 178%.** Podobnie jak w poprzednich latach najczęściej zgłaszanym incydentem było oszustwo komputerowe typu phishing. Takich incydentów było aż 25 625, co stanowi 64% wszystkich incydentów obsłużonych w 2022 r. przez CERT Polska.

1,6 mld dolarów **tyle, do 2026 r., wyniosą wydatki na cyberbezpieczeństwo w skali globalnej**

10. *Raport CERT Orange Polska za rok 2022 „ Myślę, więc jestem bezpieczniejszy" - https://cert.orange.pl/raporty-cert*

TOMASZ OMELANIUK

Presales Technical Consultant / Security SME w HP Inc Polska

Prezentowany przez Związek Cyfrowa Polska Raport pokazuje w sposób bardzo przystępny zarówno zagrożenia z jakimi się spotykamy na co dzień, ale też trendy, oraz to, w jakim kierunku zagrożenia które obserwujemy na co dzień, będą potencjalnie ewaluowały. Przytoczone w Raporcie statystyki są porażające, ale bardzo dobitnie pokazują, iż Polska na tle świata nie jest żadnym wyjątkiem od reguły. Poszczególne wartości procentowe mogą się co prawda różnić, jednakże na koniec dnia przekaz jest jeden: nikt, ale to absolutnie nikt, nie powinien czuć się bezpiecznie, jeśli chodzi o szeroko pojęte zagadnienie cyberbezpieczeństwa. Nieważne, czy jesteśmy Janem Kowalskim, małym urzędem, czy też wielką korporacją wydającą rocznie miliony dolarów na zapewnienie bezpieczeństwa. Każdy z nas prędzej czy później zostanie dotknięty tym problemem i na własnej skórze przekona się, iż „bezpieczeństwo", to nie jest slogan, hasło marketingowe, wielomilionowy biznes, ale przede wszystkim coś, o czym zawsze powinniśmy pamiętać oraz ciągle się o nie troszczyć. Dlaczego? Ponieważ zagrożeń, z którymi musimy się mierzyć każdego dnia jest co raz więcej. Te najważniejsze również zostały przywołane w niniejszym Raporcie. Pamiętajmy, że cyberbezpieczeństwo to nie tylko dochodowy biznes dla firm zajmujących się rozwijaniem i wdrażaniem różnego rodzaju rozwiązań z zakresu ochrony, ale przede wszystkim okazja do zarobku dla całej masy organizacji przestępczych, ale też nie tylko.

W ostatnich latach niejednokrotnie byliśmy świadkami ataków hakerskich nie tylko na lotniska, szpitale, różnego rodzaju urzędy, banki, czy globalne korporacje. Doskonale też znamy przykłady ataków na infrastrukturę, której skutkiem były krótsze bądź dłuższe przestoje w dostępie do podstawowych usług, czy wręcz blackouty dotykające swoim zasięgiem tysiące ludzi. Dlatego tak ważne jest, aby współpracować, budować świadomość, uczyć się na błędach, a także umieć wyciągać konstruktywne wnioski i przede wszystkim czerpać jak najwięcej dobrych praktyk, o których również Raport Cyfrowej Polski wspomina. To, co również jest niezwykle ważne to, aby nie tylko wdrażać procedury bezpieczeństwa w naszych organizacjach, ale przede wszystkim, aby je stosować!

2. Jak zadbać o cyberbezpieczeństwo – zalecenia i narzędzia

2.1. Jak ochronić swój telefon przed cyberprzestępcami?

Współcześnie telefon to więcej niż urządzenie służące międzyludzkiej komunikacji. To także narzędzie do nauki, rozrywki, załatwiania urzędowych spraw, a także do prowadzenia biznesu. Dzięki dostępowi do sieci internet, z każdego miejsca na świecie możemy się komunikować, płacić rachunki, robić zakupy, a także udzielać się w mediach społecznościowych. Smartfony odgrywają w naszym życiu – zarówno osobistym, jak i zawodowym – coraz ważniejszą rolę. Dlatego muszą być dobrze chronione. Zatem ważne jest, aby:

1. **Pobierać aplikacje tylko z autoryzowanych sklepów**, takich jak Google Play (w przypadku telefonów z systemem Android), AppStore (dotyczy telefonów Apple), a jeśli chodzi o telefony Samsung – z Galaxy Store. Komunikat na ekranie „Czy na pewno chcesz skorzystać z nieautoryzowanego zasobu?", powinien powstrzymać nas przed instalowaniem nieznanego oprogramowania.
2. **Tworzyć kopie zapasowe danych w chmurze**, co może zabezpieczyć przed utratą dostępu do danych w przypadku zagubienia, kradzieży lub zniszczenia telefonu. Dzięki temu żadne pliki nie zostaną bezpowrotnie utracone.
3. **Korzystać z systemów antywirusowych**, co jest tak samo ważne jak w przypadku komputerów i laptopów. Niestety, niewiele osób zdaje sobie sprawę, że smartfon jest takim samym urządzeniem osobistym, tak samo narażonym na cyberzagrożenia.
4. **Korzystać z managera haseł**, czyli aplikacji (często wbudowanej w przeglądarkę internetową), za pomocą, której można generować bardzo silne hasła (np. losowe ciągi znaków) oraz przechowywać je w bezpiecznej formie. Manager haseł pozwala na automatyczne uzupełnianie pola logowania oraz hasła dla konkretnych stron/aplikacji, co zwalnia z konieczności zapamiętywania tych informacji przez użytkownika.

5. **Korzystać z możliwości zdalnego wymazywania danych** na telefonie w przypadku zagubienia, co stanowi ważny element ochrony naszej prywatności.

6. **Używać aplikacji zabezpieczających** jako podstawy cyberhigieny. Jest wiele metod zabezpieczenia dostępu do telefonu – kod pin, biometria, pattern block (czyli ręczne blokowanie telefonu za pomocą odpowiedniego ruchu palca po ekranie), których ustawienie zajmuje niewiele czasu, a może uratować przez zhakowaniem.

7. **Stosować różne hasła do różnych aplikacji i kont.** Dlaczego? Bo jeśli dojdzie do zhakowania jednego konta, to stracimy wszystkie dane i informacje ze wszystkich kont – cyberprzestępca za pomocą jednego hasła zaloguje się do wszystkich portali.

8. **Budować świadomość cyberbezpieczeństwa**, zaczynając od siebie i swoich najbliższych. Wcale nie musimy pełnić ważnej funkcji publicznej, aby wiedzieć, że zawsze warto dbać o swoje urządzenie i je oraz umieszczone w nim dane chronić.

9. **Posiadać aktualny system operacyjny**, bo aktualizacja oznacza, że wykryto luki bezpieczeństwa w oprogramowaniu i zdecydowano się na ich likwidację. To ważne zarówno dla biznesu, jak i prywatnego użytkownika. W przypadku korzystania z telefonów firmy Samsung warto używać Samsung Knox, czyli platformy, która w dodatkowy sposób chroni dane wrażliwe.

10. **Korzystać z uwierzytelnienia dwuskładnikowego**, czyli na przynajmniej dwóch poziomach. Może to być np. hasło, kod sms, potwierdzenie logowania się na urządzeniu za pośrednictwem maila. To dodatkowo utrudnia potencjalnemu cyberprzestępcy wykradanie danych.

11. **Stosować VPN**, czyli wirtualną sieć prywatną (ang. virtual private network), która pozwala zachować prywatność w przypadku przeglądania internetu. Szczególnie jest to ważne przy korzystaniu z sieci Wi-Fi.

12. **Ładować telefon za pomocą własnych powerbanków**, bowiem korzystanie z ładowarek w miejscach publicznych może przyczynić się do zhakowania urządzenia.

13. **Oddzielać życie prywatne od zawodowego.** Jest to o tyle ważne, że na firmowym urządzeniu może znajdować się znacznie więcej danych wrażliwych, niż nawet w przypadku prywatnych informacji o danej osobie. Dlatego warto stosować sprzęt zgodnie z jego przeznaczeniem – telefon prywatny do spraw prywatnych, a służbowy – do zawodowych.

2.2 Jak sprawdzić bezpieczeństwo oprogramowania w internecie?

Użytkownicy internetu codziennie pobierają setki tysięcy programów komputerowych, gier i aplikacji. Większość z nich dostępna jest na autoryzowanych platformach gamingowych, zaufanych serwisach internetowych lub platformach dystrybucji takich jak AppStore, MicrosoftStore czy GooglePlay. W przypadku korzystania z programów z zaufanych źródeł, ryzyko pobrania zainfekowanego lub złośliwego oprogramowania jest niemalże równa zeru. To dzięki temu, że dystrybutorzy programów i aplikacji stosują rygorystyczne zasady bezpieczeństwa, jakie muszą spełniać gry czy programy, zanim zostaną na dopuszczone do dystrybucji. Zupełnie inaczej jest w przypadku oprogramowania dostępnego za pomocą stron internetowych. Tutaj na użytkowników czyhają różne zagrożenia, a ryzyko pobrania wirusa razem z programem jest często wysokie. Dlatego:

1. **Nie pobieraj programów z nieznanego źródła**

   – przed pobraniem oprogramowania, zawsze dokładnie sprawdź stronę, z której go pobierasz. **Pobieraj oprogramowanie jedynie z zaufanych źródeł i autoryzowanych sklepów czy platform.** Nigdy nie korzystaj ze stron internetowych, które mają literówki w adresie www lub takich, które są niezabezpieczone. Nie ufaj też programom kryjącym się pod linkami, które otrzymujesz od nieznanych osób lub w łańcuszkach internetowych.

2. **Unikaj nieznanych wydawców i autorów (Unknow Publisher)**

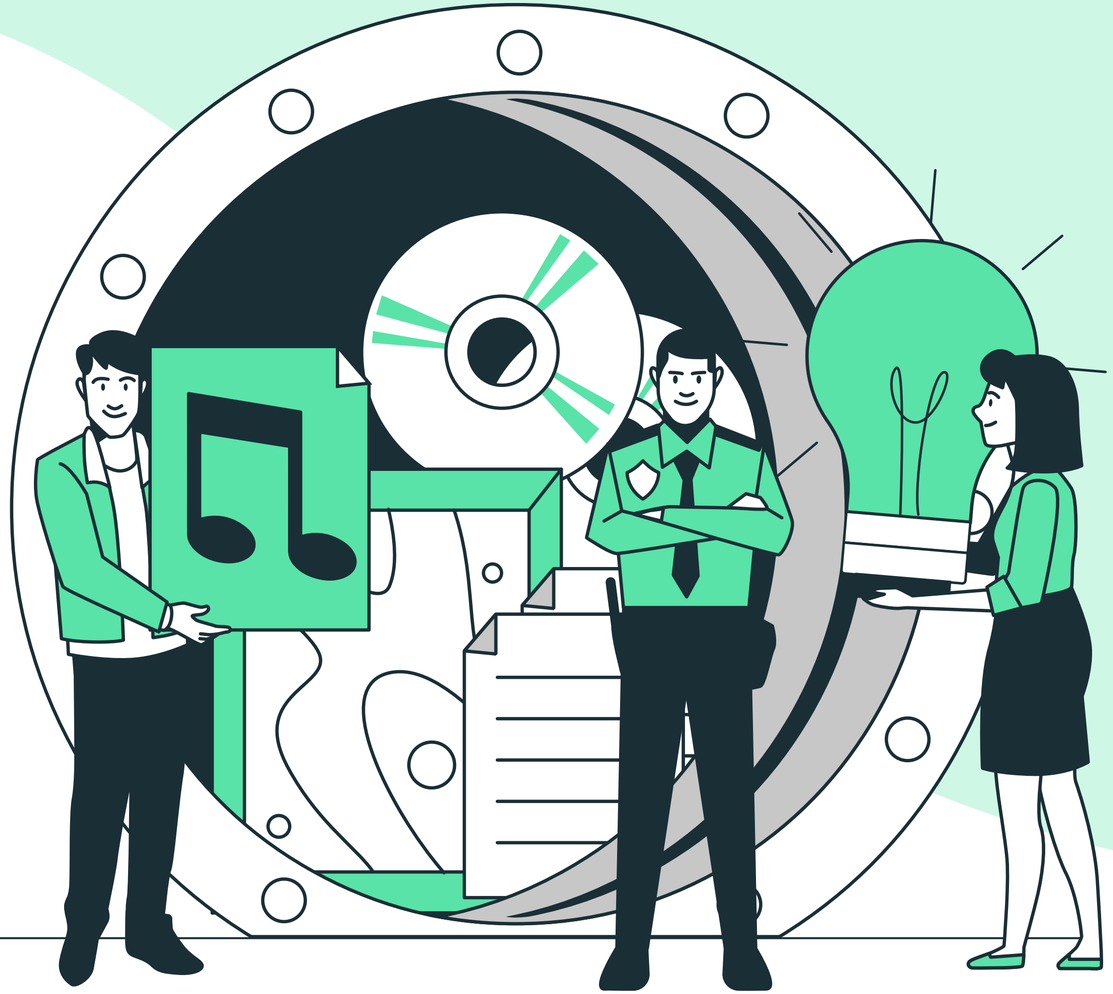
   – pobierając program w internecie, musisz wyrazić zgodę na jego instalację. Na początku każdej instalacji pojawia się charakterystyczne okno, która zawiera najważniejsze informacje o oprogramowaniu. Podstawową rzeczą, na którą powinieneś zwrócić uwagę, jest autor oprogramowania. **Jeśli w polu „autor” widnieje Nieznany Wydawca, potraktuj to jako pierwsze ostrzeżenie.** Oznacza to, że jego właściciel nie jest zaufanym publicznie wydawcą, i nie został pozytywnie zweryfikowany przez Urząd Certyfikacji i nie uzyskał certyfikatu Code Signing. Nie musi to koniecznie oznaczać, że oprogramowanie jest szkodliwe, ale z pewnością wskazuje, że jego autor nie zadbał w odpowiednim stopniu zarówno o sam kod, jak i jego użytkowników.

3. **Korzystaj z filtru Windows SmartScreen**

   - wbudowanego narzędzia systemowego, uruchamianego automatycznie, które sprawdza przeglądane witryny i programy pobrane z Internetu. **Jeśli wykryje coś podejrzanego, wyświetli użytkownikowi stronę z ostrzeżeniem, a w przypadku programów komputerowych - stronę informującą o potencjalnie szkodliwym oprogramowaniu.** Jeśli wydawca oprogramowania nie jest zaufany, a system ostrzega przed instalacją programu ekranem SmartScreen, lepiej zrezygnować z jego pobierania.

4. **Sprawdzaj certyfikaty oprogramowania.**

   Certyfikat oprogramowania, czyli Code Signing, to narzędzie umożliwiające podpisanie kodu oraz jego ochronę przez niechcianą modyfikacją. Oznacza to, że pobierając podpisane certyfikatem Code Signing oprogramowanie od Zaufanego Wystawcy zyskujesz pewność, że nie zostało ono zainfekowane czy zmienione od momentu publikacji. **Jak sprawdzić certyfikat oprogramowania?** Zanim zainstalujesz program, kliknij prawym przyciskiem myszy na jego ikonę i wybierz „Właściwości". Wyświetli się okno zawierające wszystkie niezbędne informacje o oprogramowaniu oraz jego podpisie cyfrowym. Będziesz mógł nie tylko podejrzeć, skąd i od kogo pochodzi oprogramowanie, ale uzyskasz również datę jego podpisu oraz wszystkie niezbędne informacje, jakie potrzebujesz, aby mu zaufać. **Jeśli masz taką możliwość, zawsze sprawdzaj certyfikat Code Signing oprogramowania.** Cyfrowe certyfikaty pełnią w Internecie rolę dowodów osobistych, które identyfikują kod oraz na jego podstawie umożliwiają mu dystrybucję na popularnych i zaufanych platformach.



2.3 Jak bezpiecznie korzystać z sieci?

W korespondencji mailowej używaj Certyfikatu S/MIME!
W czasie pandemii i lockdownu wzrosła popularność komunikacji elektronicznej i nie zanosi się na to, że będzie słabnąć. Przez e-mail rezerwujemy hotele, zgłaszamy reklamacje czy kontaktujemy się z urzędami. Jednak czy mamy pewność, że te dane są odporne na przejęcie przez obcych ludzi, którzy wykorzystają je do kradzieży naszych pieniędzy czy zaciągnięcia kredytów? Jeżeli poczta nie jest szyfrowana, a w dodatku łączymy się z publiczną siecią wifi, jesteśmy narażeni na podsłuchanie naszej korespondencji i kradzież danych. Gdy chcemy zachować poufność przesyłanej korespondencji, **najlepszą opcją jest użycie S/MIME**, który skutecznie zaszyfruje wiadomości. Dzięki certyfikatowi tylko adresat odczyta ich treść. **S/MIME gwarantuje, że odbiorca wiadomości otrzyma ją w formie niezmienionej i zabezpieczonej** przed odczytaniem przez nieuprawnione osoby, a także, że e-mail pochodzi faktycznie od osoby, która widnieje w polu nadawcy.

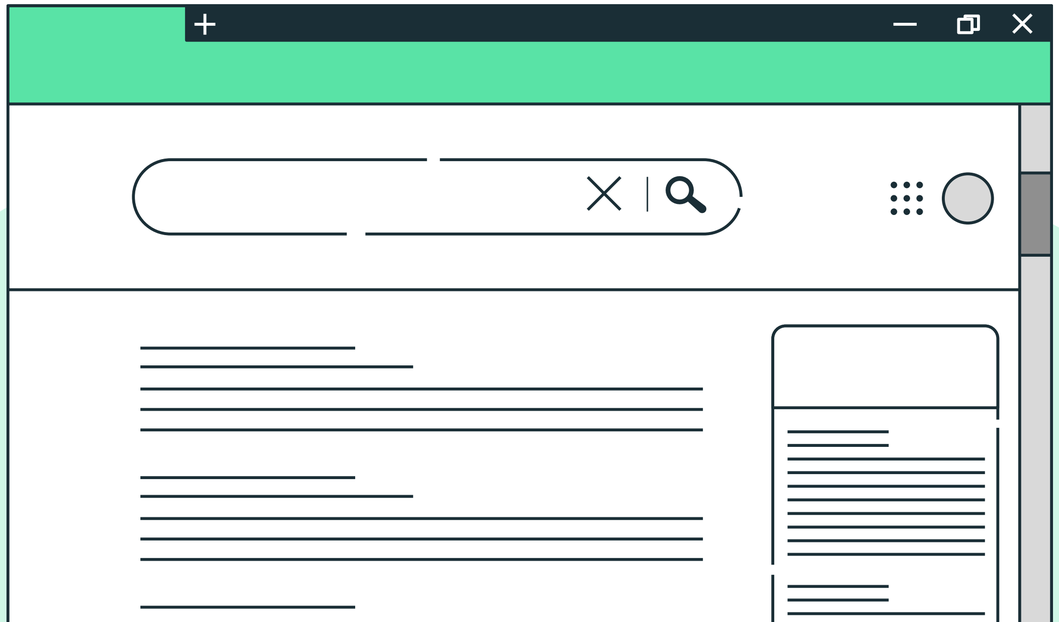
Sprawdź, czy jest kłódka w adresie strony!
Kłódka w przeglądarce internetowej widoczna przed adresem www to symbol certyfikatu bezpieczeństwa SSL. Strony internetowe bez odpowiednich zabezpieczeń są łatwym łupem dla cyberprzestępców. Można na nich odczytać nie tylko zamieszczone treści, ale również dane, które są przekazywane przez użytkowników w przypadku strony banku czy sklepu internetowego. Jeśli witryna nie jest odpowiednio zabezpieczona to wszystkie dane do logowania, w tym hasła, są narażone na ujawnienie. Po tych kłódkach możemy sprawdzić czy właściciel danej witryny odpowiednio ją zabezpieczył i czy możemy mu ufać. Brak certyfikatu SSL odbija się niekorzystnie również na pozycjonowaniu strony w wyszukiwarkach. Odwiedzający po wejściu na taką stronę zobaczy informację, że jest ona niezabezpieczona, co z pewnością zniechęci go do dalszego przeglądania.

Certyfikaty SSL są wydawane po przedstawieniu przez właściciela witryny szeregu dokumentów potwierdzających istnienie organizacji, prawo do domeny oraz uprawnienia osoby starającej się o certyfikat do reprezentowania firmy.

Na co zwracać uwagę przy przeglądaniu strony www?

W dzisiejszych czasach dbałość o bezpieczeństwo w Internecie rozwinięta jest już na tyle, że przeglądarka sama powiadomi użytkownika o braku certyfikatu SSL na danej stronie. Zdarzają się niestety i tutaj oszustwa i nie zawsze certyfikat jest gwarancją, że strona jest prawdziwa. Istnieje jednak wiele sposobów, aby ustrzec się przed oszustwem:

- **zwracaj uwagę na pasek adresu** - na pierwszy rzut oka może to być subtelna zmiana, na przykład jednej litery: zamiast domena.pl, oszuści użyją nazwę domeną.pl lub donnena.pl,
- w treści strony często znajdują się **błędy literowe lub językowe**,
- **sprawdzaj opinie o sklepie internetowym przed zawarciem transakcji,**
- **nigdy nie podawaj kodu cvv karty kredytowej ani jej salda,**
- **korzystaj z wirtualnych portfeli (e-portfeli), przedpłaconych kart płatniczych lub wirtualnych kart jednokrotnego użycia**
- **nigdy nie podawaj więcej danych niż jest to wymagane do zawarcia transakcji,**
- **jeżeli znajdziesz stronę wyłudzającą dane lub podejrzewasz oszustwo - zgłoś domenę do Centrum Certyfikacji, które go wydało** – certyfikat zostanie unieważniony w ciągu 24 godzin od zgłoszenia.
- możesz sprawdzić okres ważności certyfikatu – maksymalny okres ważności to 398 dni,
- sprawdź, jakie dane znajdują się w certyfikacie – jeżeli jest ich więcej niż tylko domena, oznacza to, że wniosek o certyfikat przeszedł szerszą weryfikację,



Bezpiecznie potwierdzaj swoją tożsamość w sieci!
Rozwiązania związane z identyfikacją elektroniczną funkcjonują prawie od początku Internetu. Już pierwsze serwisy poczty elektronicznej, sklepy czy fora internetowe wymagały potwierdzania tożsamości, nawet w formie deklaracji użytkownika, poprzez stworzenie loginu i hasła. Z czasem, wraz ze zmieniającymi się potrzebami usług oraz innymi serwisami, z których korzystaliśmy, zmieniały się również systemy i środki zdalnej identyfikacji elektronicznej.

Dzięki wprowadzonym przepisom znacząco zmieniły się zarówno usługi zaufania, jak i systemy identyfikacji elektronicznej w Unii Europejskiej. **eIDAS wprowadził szereg wymagań dotyczących bezpieczeństwa w zakresie zarządzania, organizacji, ale także wydawania środków identyfikacji i zarządzania systemami identyfikacji elektronicznej**. Podejście to uregulowało rynek i wprowadziło jednolite kryteria, które pozwalają na ocenę bezpieczeństwa systemów identyfikacji elektronicznej. Każdy kraj UE posiada swój węzeł, do którego podłącza swoje systemy oferujące usługi oraz dostawców środków identyfikacji. Węzły krajów są połączone ze sobą. Dzięki temu, chcąc zrealizować usługę np. w Niemczech można użyć francuskiego środka identyfikacji.

Jednym z przykładów rozwiązań agregujących różne metody zdalnej identyfikacji osoby fizycznej, jest e-ID HUB proponowany przez Asseco Data Systems. Podejście przyjęte do budowy platformy e-ID HUB stara się odpowiadać na problemy związane z bezpieczeństwem systemów potwierdzania tożsamości. Prace przy e-ID HUB są w dużej mierze ukierunkowane na **budowę modułu analizy i oceny ryzyka dla różnych systemów potwierdzania tożsamości, w tym np. wideoweryfikacji.** Docelowo również mogącej objąć dostawców środków identyfikacji, nie tylko tych podlegających Rozporządzeniu eIDAS.

W ciągu najbliższych lat nastąpi spopularyzowanie usług identyfikacji elektronicznej oraz ułatwienie korzystania z nich bez konieczności – jak jest to dzisiaj - używania kart kryptograficznych, które **zostaną zastąpione telefonem komórkowym posiadającym aplikację tzw. portfela.** W nim przechowywane będą dane użytkownika, jego atrybuty. Jest to model SSI – Self Sovereign Identity, w którym użytkownik końcowy ma wpływ na to, komu i jakie dane osobowe udostępnia. W takich sytuacjach identyfikacja elektroniczna i zakres potwierdzanych lub przekazywanych danych również może być skrojony pod potrzeby specyficznej usługi, z dużym udziałem oraz wyraźną zgodą użytkownika.

ROBERT POZNAŃSKI

Analityk, Zespół Usług Zaufania, Asseco Data Systems

Raport pokazuje, że ryzyka związane z przejmowaniem lub fałszowaniem tożsamości są istotnym zagrożeniem. Fałszywe tożsamości mogą być wykorzystywane w różnych celach, np. kradzieży pieniędzy, zawierania umów lub pozyskiwania danych osobowych. Dzisiaj, dzięki różnym działaniom uwzględniającym wymagania np. RODO, eIDAS, a także NIS2, bezpieczeństwo danych i świadomość użytkowników są o wiele wyższe, niż kilka lat temu. Usługi potwierdzania tożsamości są jednak krytyczne z uwagi na fakt, że użytkownik chce w sposób bezpieczny i niezawodny zrealizować usługę poprzez wygodne dla niego i znane narzędzia, a dostawca usług, np. bank, centrum certyfikacji lub inny podmiot, oczekuje potwierdzenia tożsamości swojego potencjalnego klienta z zapewnieniem, że nie doszło do fałszerstwa lub przejęcia tożsamości.

Cyberprzestępcy, podszywając się pod różne osoby, stosują coraz bardziej wyrafinowane metody. Np. maski, techniki mające na celu upodobnienie do innej osoby lub mechanizmy deep fake, które manipulują transmisją audiowizualną, tworząc obraz innej osoby niż ta, która stoi przed kamerą. To odwieczny wyścig zbrojeń – tworzenia zabezpieczeń i prób ich łamania. Zbudowany przez Asseco Data Systems e-ID HUB jest rozwiązaniem podnoszącym bezpieczeństwo w usługach potwierdzania tożsamości. Umożliwia on, poza wykorzystaniem dobrze znanych mechanizmów, tworzenie dedykowanych scenariuszy potwierdzania tożsamości łączących usługi różnych dostawców. Dobór usług następuje na podstawie mechanizmów ciągłej analizy i oceny ryzyka. Dzięki temu scenariusze te mogą odpowiadać na konkretne potrzeby biznesowe, preferencje użytkowników, ale przede wszystkim identyfikować słabości dostawców i dobierać ich usługi w sposób podnoszący bezpieczeństwo całego procesu. Co ważne, zastosowane w e-ID Hub algorytmy uwzględniają przeciwdziałanie atakom, które już w niedalekiej przyszłości mogą nastąpić z wykorzystaniem komputerów kwantowych. Zdecydowaliśmy się na implementację nowych algorytmów kryptograficznych, które według najnowszych badań prowadzonych przez NIST gwarantują odporność na ataki wykorzystujące moce obliczeniowe komputerów kwantowych.

Zaufaj usługom zaufania!
Usługi zaufania, takie jak kwalifikowany podpis elektroniczny czy walidacja, stanowią podstawę bezpieczeństwa procesów gospodarczych, zarówno na poziomie mikro, jak i makro. Uwierzytelniają i zapewniają integralność cyfrowych dokumentów, minimalizują ryzyka biznesowe związane z zapewnieniem bezpieczeństwa i przetwarzaniem informacji. Są też gwarantem ich zgodności z obowiązującym prawem. Należy bowiem pamiętać, że procesy biznesowe nie składają się z pojedynczych transakcji, a z sekwencji działań i przepływów w relacjach B2B, B2C, B2A i innych oraz procesów wewnętrznych w firmach.

Czym są usługi zaufania?
Usługi zaufania stanowią kluczowy element idei biznesu bez papieru. Wśród nich wyróżnia się kwalifikowane usługi zaufania, które mają największą moc prawną i są świadczone przez kwalifikowanych dostawców. Dostawca taki musi spełniać wymogi wskazane w unijnym Rozporządzeniu eIDAS z dnia 23 lipca 2014 r. Określa ono zasady stosowania usług zaufania w ujęciu transgranicznym w krajach europejskich, zapewniając ich bezpieczeństwo. Rejestr dostawców dostępny jest na stronie Narodowego Centrum Certyfikacji.

Katalog usług zaufania zawiera między innymi:

PODPIS ELEKTRONICZNY

– to dane elektroniczne używane przez osobę fizyczną jako podpis. Narzędzie to pozwala zatwierdzić dokumenty w postaci elektronicznej, eliminując tym samym potrzebę ich drukowania i wysyłania. **Istotnym jest, że podpis musi być użyty świadomie i być powiązany z podpisywanym dokumentem.** Definicja e-podpisu mieści w sobie jego różne rodzaje w zależności od mocy prawnej poszczególnych typów podpisu, np.:

- **kwalifikowany podpis elektroniczny** – daje pewność, że nikt nie ingerował w treść dokumentu, wiarygodnie identyfikuje tożsamość podpisującego, przypisany tylko podpisującemu, utworzony za pomocą bezpiecznego urządzenie o składania podpisu, równoważny z podpisem własnoręcznym, rozpoznawalny we wszystkich krajach UE.
- **zaawansowany podpis elektroniczny** – daje pewność, że nikt nie ingerował w treść dokumentu, wiarygodnie identyfikuje tożsamość podpisującego, przypisany tylko podpisującemu.
- **zwykły podpis elektroniczny** - dane w formie elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi elektronicznymi i które służą jako metoda uwierzytelniania. Takim podpisem jest choćby wpisane imię i nazwisko w treści maila.

KWALIFIKOWANĄ PIECZĘĆ ELEKTRONICZNĄ

– czyli cyfrowy odpowiednik pieczątki firmowej. Zawiera nazwę, adres i inne dane przedsiębiorstwa. Zapewnia integralność i autentyczność dokumentów elektronicznych. Narzędzie to przeznaczone jest dla osób prawnych, a więc firm, organizacji czy instytucji. Istotnym jest, że e-pieczęć umożliwia automatyzację wielu procesów związanych z dokumentami. Wdrożenie pieczęci elektronicznej można zastosować do masowej korespondencji do klientów np. w przypadku zmian naszych regulaminów lub cennika. **Dokumenty opatrzone taką pieczęcią są wiążące i potwierdzają wiarygodność nadawcy, a jednocześnie umożliwiają zaoszczędzenie na druku i wysyłce.**

KWALIFIKOWANĄ USŁUGĘ REJESTROWANEGO DORĘCZENIA ELEKTRONICZNEGO

(e-Doręczenia) – która jest równoważna prawnie z „tradycyjną" pocztową przesyłką poleconą za zwrotnym potwierdzeniem odbioru. Działa na rynku polskim i europejskim. Przy zagwarantowaniu poufności, a także z zapewnieniem dowodów wysłania i otrzymania, umożliwia przesłanie korespondencji drogą elektroniczną. **Chroni przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub nieupoważnioną ingerencją w treść korespondencji.**

KWALIFIKOWANĄ KONSERWACJĘ

– usługę zapewniającą długookresową moc dowodową ważności podpisów i pieczęci elektronicznych oraz ich jednoznacznego powiązania z treścią konkretnych dokumentów. Dzięki zastosowaniu odpowiednich środków formalno-prawnych oraz zaawansowanych metod kryptograficznych **zagwarantowana jest odporność na manipulacje (fałszerstwa) mimo ciągłego postępu technologii cyfrowych i kwantowych.**

KWALIFIKOWANY ELEKTRONICZNY ZNACZNIK CZASU

– odpowiednik daty pewnej w rozumieniu kodeksu cywilnego, czyli **poprzez powiązanie z konkretnym dokumentem wskazuje na wiarygodny czas jego powstania i dodatkowo zabezpiecza integralność jego treści.**

KWALIFIKOWANĄ WALIDACJĘ

– usługę, która wystawia poświadczenia stanowiące na mocy unijnego prawa **dowód potwierdzający ważność oraz status prawny podpisów i pieczęci elektronicznych, którymi opatrzone są dokumenty elektroniczne.** Stanowi gwarancję, że dokument nie został podrobiony.

IDENTYFIKACJĘ ELEKTRONICZNĄ

– czyli proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną, prawną lub osobę fizyczną reprezentującą osobę prawną. Pomaga „domknąć" wachlarz usług zaufania poprzez połączenie ich z tożsamością danej osoby. **Dzięki temu wiele procesów odbywających się w biznesie czy administracji publicznej może zostać przeniesionych do wymiaru cyfrowego, zapewniając wygodę użytkownikom.** Identyfikacja elektroniczna pozwala uniknąć podszywania się i modyfikacji tożsamości. Jej podstawą są nasze dane zawarte w środku identyfikacji elektronicznej – jednostce, w której znajdują się dane pozwalające na identyfikację danej osoby, przekazywane za zgodą tej osoby do strony, która tej identyfikacji potrzebuje.

Nieznajomość regulacji prawnych, a stąd niepewność co do bezpieczeństwa dokumentów elektronicznych, zniechęca wiele osób i firm do korzystania z podpisów elektronicznych i innych usług zaufania. To najważniejszy problem, bo dzisiaj nie stanowią już problemu takie kwestie praktyczne, jak dostępność i łatwość obsługi (intuicyjność) procesów paperless.

Znaj cyberprawo!

Jesteśmy świadkami przełomowego okresu w rozwoju cywilizacyjnym. Stale postępujący rozwój w dziedzinie technologii, a przede wszystkim informatyki, sztucznej inteligencji, robotyki przyczynia się do powstania nowych cyberzagrożeń nie tylko dla społeczeństw, ale też dla poszczególnych państw. Naturalnym instrumentem ochrony przed zagrożeniami jest próba stworzenia właściwych wymogów bezpieczeństwa przez prawo. W chwili obecnej w Polsce, jak i w Unii Europejskiej trwają pracę nad ponad 50 aktami prawnymi, które zaliczają się do prawa nowych technologii. Dotyczą one różnych obszarów merytorycznych związanych z nowymi technologiami, to m.in. cyberbezpieczeństwo, zarządzanie danymi, własność intelektualna. Polska, jako członek Unii Europejskiej, dołączyła do tego projektu, jak też do inicjatywy Parlamentu Europejskiego „Droga ku cyfrowej dekadzie", która ma na celu przyspieszenie transformacji cyfrowej w Europie do 2030 roku. W ramach tych i innych projektów nasz kraj musi zaimplementować szereg regulacji prawnych. Poniżej znajdują się najważniejsze zmiany z 2022 roku w związanych z cyberbezpieczeństwem aktach prawnych: NIS2, DORA, ISO 27002:2022.

ISO 27002:2022

Norma ISO/IEC 27002 została ustanowiona jako Polska Norma (choć w wersji anglojęzycznej) i przyczyniła się do aktualizacji poprzedniej wersji ustanowionej 9 lat wcześniej.

Zawiera przede wszystkim wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem i utrzymaniem Systemu Zarządzania Bezpieczeństwem Informacji. Zmodyfikowane normy zmniejszyły liczbę kategorii zabezpieczeń (metod kontrolnych) z 14 sekcji na 4, czyli obecnie mamy podział na dziedziny: organizacyjne, dotyczące ludzi, fizyczne i technologiczne. Zmniejszeniu uległa też liczba zabezpieczeń środków, które modyfikują ryzyko: z 114 na 93. Nowelizacja ISO dotyczy wszystkich podmiotów, które:

- zamierzają dokonać certyfikacji na zgodność z ISO/IEC 27001:2022,
- posiadają już certyfikat zgodności z ISO 27001:2013 i zamierzają dokonać ponownej certyfikacji na zgodność z nową normą ISO/IEC 27001:2022,
- są w trakcie certyfikacji zgodności z ISO 27001:2013 i będą musiały w przyszłości dokonać ponownej certyfikacji na zgodność z nową normą ISO/IEC 27001:2022. **Organizacje mają trzy lata na dostosowanie swoich systemów zarządzania do nowych wytycznych, czyli do 31 października 2025.**

Digital Operational Resilience Act (DORA)

Rozporządzenie DORA powstało z inicjatywy Komisji Europejskiej i dotyczy cyfrowej odporności operacyjnej dla sektora usług finansowych. DORA oznacza wiele obowiązków dla podmiotów finansowych, ale też dla firm, które dostarczają im technologie. Wspomniany akt nakłada na zarząd spółek odpowiedzialność za bezpieczeństwo operacyjne i ściśle określa wymagania dotyczące relacji z dostawcami usług ICT. Nacisk położono między innymi na obowiązki sprawozdawcze firm zewnętrznych, prawa dostępu i audytu, dostęp oraz odzyskiwanie danych. Podmioty finansowe mają też obowiązek przeprowadzania analizy i oceny ryzyka przed zawarciem umowy z dostawcą usług ICT, a swoich klientów będą musiały informować o incydentach. Za niedostosowanie się do postanowień Rozporządzenia przewidywane są kary: dla instytucji finansowych może to być nawet 10% rocznego obrotu, a dla dostawców 1% średniego dziennego światowego obrotu. Wysokość kar zależy od stopnia przewinienia. W akcie zawarto 24-miesięczne vacatio legis, więc nowe prawo **zacznie obowiązywać od początku 2025 roku**, jednak już teraz sektor finansowy powinien zacząć się przygotować do implementacji rozporządzenia. Pełne zapoznanie się z Rozporządzeniem jest wyzwaniem dla specjalistów ds. cyberbezpieczeństwa, analityków, prawników, ale też zarządów spółek, które bezpośrednio są wskazane jako odpowiedzialne za procesy bezpieczeństwa.

NIS2

NIS2 stanowi aktualizację unijnych przepisów cyberbezpieczeństwa z 2016 roku znanych jako NIS, a w Polsce zaimplementowanych jako Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Parlament Europejski zmodernizował przepisy w odpowiedzi na dynamiczną cyfryzację życia i biznesu. Dyrektywa poszerza zakres podmiotów, które muszą być zgodne z przepisami o cyberbezpieczeństwie m.in. o sektor spożywczy, odprowadzania ścieków, czy wiele obszarów produkcji. Dyrektywa nie pozostawia też wątpliwości w zakresie podmiotowym swego obowiązywania wskazując jako właściwe kryterium wielkości lub obrotu. Ze względu na to, że duża część podmiotów objętych NIS nie wywiązywała się z obowiązków, Parlament w aktualizacji Dyrektywy przewidział możliwość nałożenia kar. Ich wysokość ich jest zależna od rodzaju podmiotu: w przypadku podmiotów kluczowych mogą to być kary do 10 mln EUR lub 2% łącznego światowego obrotu, a dla podmiotów ważnych do 7 mln EUR lub 1,4% łącznego światowego obrotu. **Podmioty określone w dokumencie mają obowiązek dostosowania polityk m.in. dotyczących sposobu przeprowadzenia analizy ryzyka, SZBI, polityki zarządzania incydentami czy też dokumentacji mającej zapewnić bezpieczeństwo łańcucha dostaw, który to łańcuch w ostatnich latach bardzo często wykorzystywany jest do ataków na konkretne organizacje.** Warto zaznaczyć, że Polska przyczyniła się do kształtowania zakresu Dyrektywy NIS2. Polscy eksperci ds. cyberbezpie-czeństwa, zgłosili potrzebę uwzględnienia w niej podmiotów publicznychoraz rozszerzenia sektorów kluczowych.

Zadbaj o pamięć w komputerze!

Jeszcze dość niedawno stosowane przez użytkowników indywidualnych w komputerach wysokiej klasy, półprzewodnikowe układy pamięci (SSD), zwane konwencjonalnie „dyskami" trafiły do głównego nurtu rozwiązań komputerowych. Dyski SSD zajmują ważne miejsce w macierzach centrów danych, obsługując aplikacje obliczeniowe o wysokiej wydajności, takie jak analiza danych, Internet rzeczy (IoT), uczenie maszynowe (ML) i sztuczna inteligencja (AI). **Firma badawcza Gartner przewiduje, że w 2026 r. dyski SSD będą stanowić 32% trafiających na rynek liczonej w eksabajtach łącznej pojemności dysków twardych (HDD) i SSD**. Stały się one podporą dla menedżerów IT chcących poprawić dostęp i wykorzystanie danych – i nie bez powodu. Dyski SSD są bardziej niezawodne niż HDD, ponieważ nie mają ruchomych części, które mogą ulec awarii. Są wytrzymałe, dzięki czemu wytrzymują upadek lub uderzenie bez utraty danych. Zużywają też mniej energii, ponieważ nic się nie „rusza" w środku. Są znacznie lżejsze (a często mniejsze) niż tradycyjny dysk twardy, więc mogą być stosowane w laptopach, małych maszynach i sieciach pamięci masowej o dużej pojemności, na mniejszej powierzchni.

Dyski SSD, zwłaszcza te o dynamicznej pamięci DRAM (dynamic random-access memory), zostały zaprojektowane do bezpiecznego przechowywania danych dzięki automatycznemu szyfrowaniu wewnętrznemu. Można je porównać do automatycznej blokady i klucza. Tylko osoba posiadająca klucz wirtualny może uzyskać dostęp do danych. Dysk SSD DRAM daje użytkownikowi poczucie bezpieczeństwa dzięki szyfrowaniu sprzętowemu, które wykorzystuje własny procesor i jest odizolowane od pozostałych dysków i zasobów w komputerze. Oznacza to, że klucze szyfrowania blokujące dane są wbudowane bezpośrednio w kontroler dysku, a nie w pamięć systemową komputera lub serwera. Oznacza to również, że na dysku SDD DRAM dane zapisywane są bez konieczności podejmowania jakichkolwiek działań przez użytkownika.

Dyski SSD są nośnikami wszystkiego – od systemów operacyjnych po aplikacje o znaczeniu krytycznym dla firmy – więc służby IT muszą mieć oko na każdy dysk SSD w centrum danych. Istnieją pomocne narzędzia, takie jak Samsung Magician19. Ten program, który można szybko opanować, pomaga użytkownikom zarządzać dyskami SSD Samsung i wykonywać różne zadania, takie jak aktualizacja oprogramowania układowego oraz optymalizacja wydajności i niezawodności dysku SSD.

CYPRIAN GUTKOWSKI

Ekspert ds. procesów bezpieczeństwa IT w ComCERT SA

Ustanowienie takich aktów prawnych jak NIS2 (Directive on Security of Network and Information Systems) i DORA (Digital Operational Resilience Act) jest przełomowym momentem w dziedzinie poprawy bezpieczeństwa infrastruktury i danych na obszarze Unii Europejskiej.

Zarówno NIS2, jak i DORA, wzmacniają zdolności organizacji do reagowania na incydenty oraz mają zapewnić skuteczną ochronę sieci i systemów teleinformatycznych. Należy podkreślić, że zgodnie z tymi regulacjami konieczne jest wypracowanie skutecznych mechanizmów monitorowania i raportowania incydentów bezpieczeństwa, a także, na co jasno wskazuje NIS2 - wzmocnienie bezpieczeństwa łańcucha dostaw. Te akty prawne wymagają, aby organizacje z ich zakresu podmiotowego dostosowały się do określonych standardów bezpieczeństwa, w tym wdrożyły środki zapobiegawcze, zarządzanie ryzykiem, audyt czy raportowanie incydentów. Dzięki temu staną się bardziej odporne na atak i będą lepiej przygotowane w przypadku wystąpienia incydentu, co w efekcie pozwoli na skuteczną identyfikację, analizę i reagowanie na zagrożenia.

Zmiany w normie ISO 27002 także mają kluczowe znaczenie dla cyberbezpieczeństwa. Jest to norma dotycząca zarządzania bezpieczeństwem informacji, która stanowi kompleksowy zestaw zasad i praktyk, mających na celu ochronę poufności, integralności i dostępności informacji w organizacji.

Wprowadzenie dyrektywy NIS2, DORA i zmian w normie ISO 27002 przynosi ogromne korzyści dla naszego świata. Zwiększa świadomość i priorytetowość zagadnień z obszaru cyberbezpieczeństwa, co jest szczególnie istotne w dobie coraz bardziej zaawansowanych i złożonych ataków. Dzięki tym regulacjom kluczowe sektory są zobowiązane do wdrożenia skutecznych środków ochrony, co bez wątpienia przyczyni się do zwiększenia poziomu bezpieczeństwa nas wszystkich.

Jednak wprowadzenie tych regulacji to dopiero pierwszy krok. Kluczowe będzie skuteczne wdrażanie, egzekwowanie i dążenie do ciągłej poprawy w obszarze cyberbezpieczeństwa. Konieczne będzie też rozwijanie współpracy między państwami członkowskimi, sektorami gospodarki oraz organami regulacyjnymi w celu skutecznego reagowania na dynamicznie zmieniające się zagrożenia. Tylko w ten sposób będziemy mogli stworzyć bezpieczny cyfrowy świat dla wszystkich.

3. Rekomendacje dla urządzeń mobilnych

3.1. Rozwiązania poprawiające bezpieczeństwo urządzeń mobilnych

Platformy bezpieczeństwa oparte na oddzielnym podsystemie sprzętowym
To dedykowane moduły z własną pamięcią i procesorem, które w oddzielnym, odizolowanym od głównego systemu operacyjnego magazynie, przechowują wrażliwe dane, takie jak hasła, dane biometryczne czy też klucze kryptograficzne (np. Blockchain). Są odporne na najbardziej dotkliwe ataki, w tym laserowe, napięciowe czy temperaturowe oraz poprzez wykorzystanie ulotu elektromagnetycznego czy impulsu elektromagentycznego.

Rozwiązania do wdrażania, konfiguracji i customizacji urządzeń
Łatwe w użytkowaniu, innowacyjne narzędzia do rejestracji usług EMM (Enterprise Mobility Management), które umożliwiają udostępnianie tysięcy urządzeń do zarządzania przedsiębiorstwem, zarówno administratorom IT, jak i użytkownikom końcowym. Pozwalają na rejestrację dowolnego urządzenia roboczego w dostępnych zasobach sieci lokalnej lub w hybrydowym środowisku chmurowym. Pełna integracja z urządzeniami typu tablet czy smartfon, z dostępnymi usługami dostawcy, zapewnia kompleksowe dostosowanie do konkretnych potrzeb, tym samym przekształcając je we w pełni skonfigurowane narzędzia biznesowe.

Rozwiązania EMM (Enterprise Mobility Management) i MDM (Mobile Device Management)
To rozwiązania oparte głównie na chmurze, zarządzające funkcjami urządzeń mobilnych do celów biznesowych. Dzięki nieskomplikowanemu UX, administratorzy IT mogą zmaksymalizować produktywność, poprzez zdalne śledzenie, zarządzanie, rozwiązywanie problemów, konfigurowanie i wysyłanie wiadomości do urządzeń. Rozwiązania EMM i MDM umożliwiają zarządzanie dowolnym urządzeniem z najbardziej popularnymi systemami: Android, iOS lub Windows 10.

Rozwiązania do zarządzania oprogramowaniem urządzeń
Zapewniają stabilność i ciągłość firmom zarządzającym dużą flotą urządzeń, poprzez zaawansowaną kontrolę nad aktualizacjami oprogramowania systemowego. Zapobiegają wszelkim niechcianym, automatycznym aktualizacjom i wdrażają je dopiero po pełnym przetestowaniu na wybranych do tego celu urządzeniach. Dzięki prostej nawigacji, dopasowują się do trybu pracy firmy i dbają o to, by wszystkie zarejestrowane urządzenia działały na odpowiednich i aktualnych wersjach systemu operacyjnego bez zakłócania ich pracy.

Rozwiązania do monitorowania statusu floty urządzeń mobilnych i analityka danych[11]

Monitorowanie statusu floty urządzeń i identyfikowanie potencjalnych problemów są możliwe dzięki kompleksowemu zbieraniu danych bezpośrednio z urządzeń mobilnych. Badanie, w jaki sposób używane są aplikacje do pracy, oraz analiza nieoczekiwanych zdarzeń, takich jak awarie, nadmierne zużycie procesora, baterii czy danych sieciowych przez aplikacje. Sprawdzanie cykli ładowania urządzeń i stanu baterii w urządzeniach mobilnych. Możliwość pobrania logów dotyczących rozłączeń z sieciami bezprzewodowymi lub użycia danych komórkowych. W razie wystąpienia anormalnych zdarzeń powiadomienie administratorów. Wszystkie te analizy mają prowadzić do zwiększenia bezpieczeństwa, oszczędności zużycia energii i poprawy użyteczności zastosowanych rozwiązań.

Rozwiązania do przeciwdziałania kradzieżom i oszustwom

Zmniejszają ryzyko finansowe operatorów, banków czy platform e-commerce oferujących sprzedaż ratalną urządzeń mobilnych, poprzez możliwość zdalnego blokowania w przypadku ich kradzieży, hakowania czy nieautoryzowanych prób ich odblokowania poprzez IMEI, oprogramo-wanie fabryczne oraz modyfikację tego oprogramowania, zachowując przy tym ich całkowitą ochronę.

Rozwiązania typu MTD (Mobile Threat Defense)

Zaawansowane rozwiązania dla urządzeń mobilnych pozwalające na pełny monitoring urządzenia oraz zainstalowanych aplikacji raportujący między innymi: jakie dane i gdzie są wysyłane oraz odbierane poprzez jakie aplikacje, i jakie sensory urządzenia są wykorzystywane w danej chwili (mikrofon, kamera, lokalizacja itd.). Oprogramowanie MTD reaguje na potencjalne zagrożenia oraz blokuje całe aplikacje lub tylko ich elementy, które mogą narazić dane na wyciek. Dzięki możliwości integracji z rozwiązaniami typu EMM/MDM, w przypadku zagrożenia, mogą zostać uruchomione wcześniej skonfigurowane odpowiedzi jak np. zablokowanie lub odinstalowanie złośliwych aplikacji, odłączenie z podejrzanej sieci, ograniczanie funkcji w celu zagwarantowania najwyższego poziomu bezpieczeństwa.

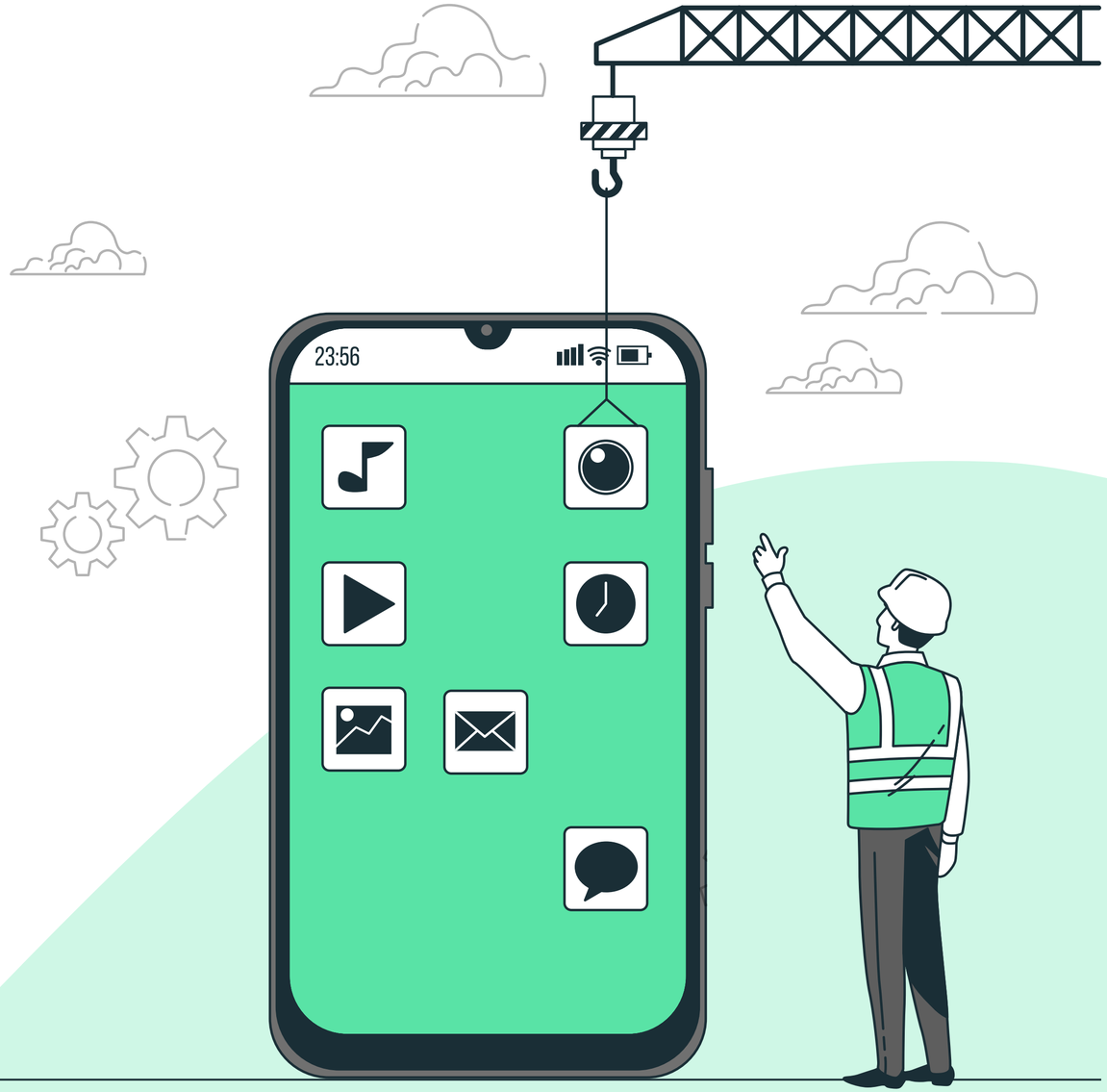
10. *Raport CERT Orange Polska za rok 2022 „ Myślę, więc jestem bezpieczniejszy" - https://cert.orange.pl/raporty-cert*

Sprawdzanie integralności urządzenia

Weryfikacja stanu urządzenia i jego integralności jest istotne z perspektywy ochrony danych, które się na nim znajdują. Nowoczesne systemy dostarczają mechanizmy, które w niekwestionowany sposób raportują status. Wymaga to integracji z infrastrukturą producenta urządzenia i często bywa częścią funkcji dostarczanych przez MDM.

Akcesoria

Obecnie urządzenia mobilne posiadają bardzo wiele zastosowań. Wśród nich możemy wymienić wiele takich, które są dla nas bardzo istotne w kontekście pracy lub codziennego życia. Niektóre funkcje mogą być nawet krytyczne dla naszego zdrowia czy bezpieczeństwa. Mówimy tu o funkcjach związanych z płatnościami mobilnymi, e-dokumentami, monitorowaniem stanu zdrowia i telemedycyną, lokalizacją w czasie rzeczywistym uruchomioną ze względów bezpieczeństwa czy choćby najprostszą możliwością kontaktu z odpowiednimi służbami w sytuacji zagrożenia. Dlatego ważnym aspektem bezpieczeństwa urządzeń jest stosowanie odpowiednich akcesoriów umożliwiających zabezpieczenie fizyczne chroniące przed zniszczeniem urządzenia (obudowy) czy dające możliwość ładowania baterii w wygodny i szybki sposób.



3.2 Certyfikacje dla urządzeń mobilnych

Common Criteria

To międzynarodowa norma definiująca kryteria oceny bezpieczeństwa systemów teleinformatycznych. Proces certyfikacji obejmuje między innymi określenie funkcjonalności bezpieczeństwa produktu, przegląd dokumentacji architektury i rozwoju produktu, a także rygorystyczne niezależne testy funkcjonalności oraz analizę luk w zabezpieczeniach, dokonywaną przez akredytowane, niezależne laboratorium testowe. Standard Common Criteria jest uznawany przez wiele organów rządowych na całym świecie, takich jak National Cyber Security Centre (Wielka Brytania), Centro Criptológico Nacional (Hiszpania), Agence Nationale de la Sécurité des Systemes d'Information (Francja), Bundesamt für Sicherheit in der Informationstechnik (Niemcy), National Security Agency oraz National Institute of Standards and Technology (Stany Zjednoczone), jak również wiele innych. Wiele rządów wymienia go wśród wymogów w przetargach dot. produktów bezpieczeństwa. Posiadanie certyfikatu CC nie gwarantuje, że produkt jest bezpieczny pod każdym względem – zapewnia jedynie o działaniu wszystkich zadeklarowanych przez producenta zabezpieczeń.

FIPS 140-2

Certyfikat FIPS 140-2, przyznawany przez amerykański Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology), jest jednym z najbardziej pożądanych na świecie certyfikatów bezpieczeństwa wobec systemów kryptograficznych, i tym samym należy do najtrudniejszych do zdobycia. Władze regionalne, stanowe i lokalne w Stanach Zjednoczonych często wymagają zgodności FIPS (Federal Information Processing Standard) w każdym produkcie zawierającym moduł kryptograficzny. Standard FIPS 140-2 określa cztery poziomy ochrony i odnosi się do wszystkich produktów służących do przechowywania lub przesyłania istotnych danych. Do produktów tych zaliczają się m.in. urządzenia do szyfrowania łączy, dyski twarde, dyski flash oraz inne wymienne pamięci masowe.

SOC2

Service and Organization Controls 2 to międzynarodowy standard gromadzenia i wymiany informacji. Standard ten powstał z ramienia Amerykańskiego Instytutu Biegłych Rewidentów (American Institute of Certified Public Accountants, AICPA). Definiuje on kryteria zarządzania danymi w kontekście pięciu kluczowych obszarów: security – bezpieczeństwo fizyczne i logiczne, availability – dostępność, processing integrity – integralność przetwarzanych danych, confidentiality – poufność, privacy – prywatność. To procedura audytowa, której efektem jest raport szczegółowo opisujący, w jaki sposób dostawca usług zarządza powierzonymi mu danymi.

TOMASZ CHOMICKI

Dyrektor ds. rozwoju biznesu w Samsung Electronics Polska

We współczesnym świecie trudno funkcjonować bez smartfona, smartwatcha czy tabletu - nie jest to oczywiście niemożliwe, ale dzięki nim załatwimy sprawy urzędowe, kupimy prezenty dla najbliższych, bilety do kina, zamówimy hotel na urlop, zmierzymy naszą aktywność fizyczną i monitorujemy nasze zdrowie. Przeczytamy newsy z każdego końca świata i jeszcze dowiemy się jaka tam będzie pogoda za kilka dni, skorzystamy z mediów społecznościowych i będziemy w ciągłym kontakcie z bliskimi, przyjaciółmi, czy też ze współpracownikami. Do tego jeszcze zachowamy mnóstwo zdjęć, filmów czy dokumentów. One dają nam szybki dostęp do naszych kont bankowych, skrzynek pocztowych i kontaktów. Te małe urządzenia czasami wiedzą o nas więcej niż my sami o sobie wiemy. A te dane i informacje o nas to najcenniejsza waluta, którą wyjątkowo trzeba chronić. Dlatego tak bardzo ważne, aby zapewnić wszystkim urządzeniom mobilnym, z których korzystamy, pełne bezpieczeństwo. Bez względu na to, do jakich celów je wykorzystujemy - czy do pracy zawodowej, czy do spraw codziennych.

Jako producent jednych z najbardziej popularnych, nie tylko w Polsce, urządzeń mobilnych, definiujemy bezpieczeństwo jako pełen zakres usług end-to-end, to znaczy, że ochrona użytkowników nie kończy się z momentem, gdy dany smartfon lub inne urządzenie trafia do ich rąk. I to bez względu na model danego urządzenia - klient jest chroniony na tym samym poziomie, niezależnie od tego czy korzysta z najnowszego czy ze starszego sprzętu.

Dodatkowo, także od strony konsumenta rośnie świadomość ochrony własnej prywatności i informacji gromadzonych w smart urządzeniach, choć nadal się zdarza, że takie dane jak adres mail, numer telefonu, a nawet numer karty kredytowej przekazywane są w przestrzeń cyfrową bez większego zastanowienia. A te padają łupem cyberprzestępców.

Od ponad 10 lat Samsung tworzy rozwiązania mobilne z platformą KNOX, które można zaliczyć do najbardziej bezpiecznych na Świecie. Samsung KNOX to coś więcej niż wbudowana w świat mobilny platforma bezpieczeństwa, która zawiera różnego rodzaju rozwiązania do pełnego zarządzania oraz kontrolę i automatyczne wdrożenia procesów.

Jest to kompleksowe rozwiązanie, które oparte o wysokospecjalistyczną platformę sprzętową zawiera klucze kryptograficzne zawarte w układach elektronicznych, zestaw oprogramowania oraz systemy chmurowe.

Idąc naprzeciw współczesnym zagrożeniom Samsung stworzył najnowszą ochronę przeciwko coraz to bardziej skomplikowanym atakom hackerskim – Samsung KNOX Voult. Jest to nowy zestaw narzędzi, oparty o izolowane, oparte na sprzęcie i wysoce bezpieczne środowisko dla najbardziej krytycznych informacji na twoich urządzeniach. Jest to rozwiązanie dedykowane do świata urządzeń Galaxy.

Samsung Knox Vault to połączenie sprzętu zabezpieczającego (nowy bezpieczny procesor i izolowana bezpieczna pamięć) oraz nowego zintegrowanego oprogramowania, które chroni najbezpieczniejsze dane przed niekontrolowanymi działaniami różnych aplikacji a nawet niepożądanymi działaniami systemu operacyjnego.

W przypadku Samsung Knox Vault skupiliśmy się na zaprojektowaniu bezpiecznego i wysoce chronionego miejsca dla naszego zaufanego oprogramowania. Jego zadaniem jest wyłącznie zarządzanie i ochrona najbardziej krytycznych informacji: kodów PIN, haseł, danych biometrycznych, certyfikatów cyfrowych, kluczy kryptograficznych i innych poufnych informacji.

Bezpieczny procesor Knox Voult działa niezależnie od głównego procesora, na którym działa system operacyjny Android, jeszcze bardziej poprawiając stan naszych zabezpieczeń i minimalizując współużytkowane komponenty w celu złagodzenia potencjalnych wektorów ataku.

We współczesnym świecie wektory ataków opartych na oprogramowaniu to nie jedyne wektory. Samsung wziął pod uwagę również „fizyczne” ataki na smartfon. Są to wyrafinowane ataki przeprowadzane przez kogoś, kto pozyskał fizycznie telefon i chce wydobyć ukryte w nim wrażliwe informacje. Gdy ktoś próbuje bezpośrednio manipulować elektroniką telefonu — na przykład za pomocą światła laserowego lub wstrzyknięcia usterki elektromagnetycznej — zabezpieczone informacje w skarbcu mogą ulec samozniszczeniu, uniemożliwiając dostęp do nich.

Przed tego typu ataki chroni nas architektura Knox Voult, która poddana jest certyfikacji cyberbezpieczeństwa common criteria na poziomie EAL 5+

3.3 Ochrona drukarek i urządzeń wielofunkcyjnych

Aby zwiększyć bezpieczeństwo drukarek i urządzeń wielofunkcyjnych należy stosować urządzenia, które:

- wyposażone są w mechanizm stałego monitorowania urządzenia na wypadek różnych ataków sieciowych, a w przypadku ich wykrycia umożliwiają wysłanie stosownego komunikatu do zewnętrznego systemu typu SIEM oraz rozpoczęcie procesu eliminacji i zniwelowania potencjalnej próby ataku,
- umożliwiają zablokowanie nieautoryzowanych prób aktualizacji oprogramowania układowego (bios/firmware) oraz wyłączenia opcji zdalnych aktualizacji, a także wyłączenie portów USB (zarówno dla wydruków z pendrive'ów, jak również bezpośrednich wydruków z komputera),
- umożliwiają definiowanie czasu, po upływie którego urządzenie będzie wylogowywało użytkownika ze strony konfiguracyjnej urządzenia,
- posiadają możliwość automatycznego wylogowania użytkownika z urządzenia po upływie pewnego czasu lub też po wykonaniu zadania,
- umożliwiają zablokowanie dla użytkowników opcji alternatywnego logowania do urządzenia, innej niż logowanie skonfigurowane jako domyślne,
- posiadają szyfrowane dyski twarde lub w przypadku ich braku odpowiednio szyfrowane miejsce, w którym przechowywane są dokumenty użytkowników – tymczasowo lub do momentu ich zwolnienia,
- posiadają możliwości zdefiniowania sposobów usuwania danych z urządzenia wraz z nadpisywaniem miejsca, w którym były one zapisane oraz posiadają mechanizm trwałego i bezpiecznego usuwania danych z dysku na żądanie,
- posiadają możliwość wymuszenia stosowania przynajmniej PIN-ów w celu wdrożenia poufności drukowanych dokumentów, a w przypadku otrzymania wydruku bez PIN-u – automatycznego jego usunięcia i pominięcia jego drukowania,
- posiadają możliwości ograniczenia i zdefiniowania docelowych domen pocztowych, na które użytkownicy będą mogli wysyłać swoje skany. Wszystkie pozostałe domeny w adresach email powinny być zablokowane i ignorowane przez urządzenie,
- posiadają wbudowaną zaporę sieciowa (firewall) lub chociaż możliwość zdefiniowania tzw. listy dostępowej (ACL), czyli komputerów lub serwerów, z których urządzenie będzie tylko przyjmowało dokumenty do wydruku,
- umożliwiają wyłączenie zbędnych i nieużywanych protokołów zarządzania urządzeniem oraz wydruku,
- posiadają wsparcie dla szyfrowanych protokołów transmisji i wydruku,
- posiadają wsparcie dla szyfrowanych protokołów SSL/TLS przy wysyłaniu zeskanowanych dokumentów na maila (SMTP),
- umożliwiają zdefiniowanie zblokowanych numerów, z których faksy nie będą odbierane,
- umożliwiają zdefiniowanie godzin, w których otrzymane faksy będą drukowane.

3.4 Ochrona laptopów i komputerów stacjonarnych

Laptop i komputer stacjonarny powinny posiadać:

- dysk z funkcją samoszyfrowania SED (self-encyption drive) zgodny ze standardem OPAL2,
- system operacyjny, dający możliwość szyfrowania dysków twardych wraz z opcją szyfrowania pamięci zewnętrznych – jak klucze USB (tzw. pendrive), zewnętrzne dyski, etc.,
- w przypadku laptopów i notebooków: wbudowaną dodatkową kamerę podczerwieni (Infra Red), pozwalającą na bezpieczne logowania do komputera za pomocą skanu twarzy (face recognition) z wykorzystaniem wbudowanej technologii Windows Hello,
- wbudowany kontroler bezpieczeństwa chroniący obszar pamięci EMM przed uruchomieniem na poziomie UEFI nieautoryzowanego kodu złośliwego, będącego wynikiem ataków typu malware,
- w przypadku laptopów i notebooków: wbudowany w wyświetlacz filtr prywatyzujący sterowany elektronicznie z klawiatury komputera, pozwalający na ograniczenie kątów widzenia do wartości +/- 45 stopni przy co najmniej 90 % spadku kontrastu,
- mechanizm ciągłego monitorowania integralności podstawowego oprogramowania układowego (BIOS), a w przypadku stwierdzenia jego „kompromitacji" uruchomienie samoczynnej procedury przywrócenia oryginalnej wersji oprogramowania zgodnie z rekomendacjami Amerykańskiego Narodowego Instytutu Standardów i Technologii (NIST),
- mechanizm zabezpieczający komputer i przywracający go do poprawnego działania w przypadku zaniku prądu w trakcie aktualizacji podstawowego oprogramowania układowego (BIOS),
- możliwość zainicjowania aktualizacji podstawowego oprogramowania układowego komputera (BIOS) poprzez mechanizm Windows Update wraz z aktualizacją systemu operacyjnego,
- rozwiązania wykorzystujące wbudowane w procesor mechanizmy wirtualizacji pozwalające otwierać w bezpieczny sposób, izolowany od podstawowego systemu operacyjnego, dokumenty bądź też odnośniki do stron, mogące zawierać elementy szkodliwego oprogramowania,
- czujnik otwarcia obudowy, zbierający informacje o zdarzeniach związanych z otwieraniem obudowy, pozwalający zdefiniować dodatkowe akcje w momencie otwarcia obudowy komputera,
- funkcjonalność bezpiecznego, trwałego usuwania danych z dysków wbudowaną bezpośrednio w BIOS,
- dedykowany, sprzętowy moduł/układ TPM na płycie głównej (ang. discrete TPM),
- mechanizmy pozwalające wdrożyć biometryczne metody identyfikacji użytkownika a tym samym zastąpić wszechobecne logowanie do systemów przy wykorzystaniu tradycyjnego hasła,

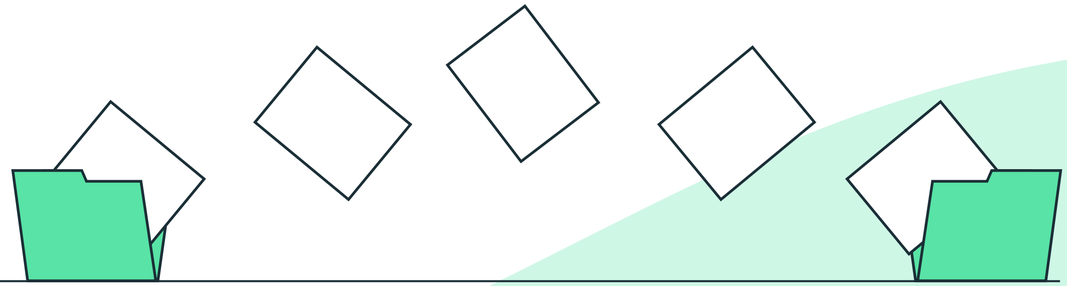
- czytnik kart inteligentnych pozwalający na wdrożenie nie tylko dodatkowego mechanizmu dwuskładnikowego uwierzytelnienia, ale też na wykorzystanie kart typu smart do podpisu elektronicznego,
- możliwość przywrócenia systemu operacyjnego w bezpieczny sposób w przypadku skutecznego ataku, czy też na skutek działania szkodliwego oprogramowania, które to spowoduje uszkodzenie systemu operacyjnego komputera, a tym samym brak możliwości jego uruchomienia,
- w przypadku używania bezprzewodowego zestawu: klawiatura i/lub mysz – z posiadanym komputerem komunikacja pomiędzy tymi urządzeniami a komputerem powinna być szyfrowana,
- możliwość zastosowania tzw. linek zabezpieczających, aby móc fizycznie zabezpieczyć urządzenia w miejscach ogólnodostępnych,
- oprogramowanie antywirusowe nowej generacji (ang. Next-Generation Antivirus - NGAV) pozwalające na bardziej precyzyjne wykrywanie nowych zagrożeń związanych z działaniem szkodliwego oprogramowania,
- aktualne oprogramowanie systemowe oraz aktualne i najnowsze wersje używanych przeglądarek internetowych oraz czytników poczty internetowej.

Podsumowanie

Dziś trudno nie mówić o cyberochronie, a także o dezinformacji, nie odnosząc się do tego, co się dzieje za wschodnią granicą Polski i Unii Europejskiej. Największym wyzwaniem dla branży w wielu krajach na świecie jest w tej chwili zapewnienie cyfrowej ochrony infrastrukturze krytycznej (m.in. transport, zdrowie, energia, finanse) przed atakami hakerów, a także społeczeństwu, przeciw któremu są wymierzane precyzyjne kampanie dezinformacyjne wprowadzające chaos i niepokój. Na celowniku cyberprzestępców jest także szeroko rozumiany biznes - od małych działalności gospodarczych, przez fabryki i zakłady przemysłowe, po korporacje międzynarodowe. Zwłaszcza, że ich rozwój nieustannie wspierają urządzenia końcowe: smartfony, tablety, laptopy, komputery stacjonarne, drukarki, czy też urządzenia wielofunkcyjne.

Stąd tak ważna jest edukacja użytkowników, która - sądząc po danych CERT NASK dotyczących zgłoszeń incydentów cyberbezpieczeństwa - przynosi już owoce (wzrost o **178%**), ale jeszcze nadal jest wiele do zrobienia. Zwłaszcza, że zawsze najsłabszym ogniwem w procesie cyberochrony jest człowiek. Stąd też w poniższym opracowaniu zawarte zostały rekomendacje i zalecenia dotyczące ochrony urządzeń końcowych, powstałe w oparciu o doświadczenie firm technologicznych, tworzących Związek Cyfrowa Polska.

Tak jak w okresie rewolucyjnych zmian technologicznych wymuszonych pandemią, tak w czasie bezprecedensowej inwazji Rosji na Ukrainę i związanymi z nią cyber atakami na niespotykaną dotąd skalę, branża cyberbezpieczeństwa na całym świecie odgrywała jedną z głównych ról, zapewniając odpowiednią cyfrową ochronę zarówno w sektorze prywatnym jak i państwowym. Ochrona cyberprzestrzeni i infrastruktury stała się priorytetem administracji państwowych i wpłynęła na zacieśnienie współpracy z branżą technologiczną. To z kolei wiązało się ze zwiększeniem inwestycji w rozwiązania i narzędzia cyberochrony, a także otworzyło jeszcze szerzej drzwi dla usług oraz produktów tworzonych przez krajowych producentów z sektora. Warto podkreślić, że dla wzmocnienia publicznego procesu zakupowego systemów IT powstały rekomendacje Prezesa Urzędu Zamówień Publicznych, które także są następstwem owocnej współpracy administracji państwowej i branży technologicznej.



Zobacz: Rekomendacje dotyczące zamówień publicznych na systemy informatyczne wydane przez Urząd Zamówień Publicznych *https://www.uzp.gov.pl/baza-wiedzy/dobre-praktyki/rekomendacje-dotyczace-zamowien-publicznych-na-systemy-informatyczne)*

Dla polskiego biznesu niezwykle istotne problemy stanowią niedobór wykwalifikowanych pracowników, a także, ze względu na inflację, koszty rozwiązań ochronnych. Obie te kwestie bez wątpienia wpływają na poszukiwanie oszczędności w budżetach. Stąd tak ważnym jest, by redukcje kosztów w jak najmniejszym stopniu dotyczyły cyberochrony, a dostęp do rozwiązań i narzędzi wypracowanych w oparciu o najnowsze technologie, oferowane przez liderów branży technologicznej, **w tym zrzeszonych w Związku Cyfrowa Polska - był jak najszerszy. W roku 2030 polska gospodarka cyfrowa ma być warta 123 mld euro, co oznacza, że usługi cyfrowe stanowić będą 9% prognozowanego PKB[12].** Jednak zanim tak się stanie, już dziś należy usuwać bariery i podejmować wyzwania na rzecz cyberochrony polskiej gospodarki i społeczeństwa.

12. *Raport „Polska jako Cyfrowy Challenger i lider handlu cyfrowego" przygotowany przez McKinsey - https://www.mckinsey.com/pl/our-insights/digital-challengers-3*