Cyberbezpieczeństwo w Polsce w 2021 r.: cyberataki na urządzenia końcowe

Raport przygotowany przez:

Warszawa, grudzień 2021 r.

Spis Treści

1. Wstęp

Tak jak przez ostatnie dwa lata, odmienianym przez wszystkie przypadki było słowo „pandemia", tak na co dzień towarzyszyło mu szeroko rozumiane „bezpieczeństwo". I tak jak z roku na rok, skala zagrożeń w wirtualnej rzeczywistości rosła, tak przez ostatnie dwa lata jej dynamika znacząco przyspieszyła. Nagłe przechodzenie gospodarek w system nauki i pracy zdalnej i hybrydowej, oraz wymuszone korzystanie z e-usług, otworzyło szerzej nie furtkę, a bramę dla działalności cyberprzestępców.

W 2021 r. aż 83% polskich firm wdrożyło w swojej działalności pracę zdalną – niemal w pełni w klasycznym modelu z wykorzystaniem służbowych laptopów i szyfrowanych połączeń (VPN), a połowa z nich jednocześnie stwierdziła wzrost podatności na cyberataki w związku z wymuszonymi zmianami organizacji pracy[1]. Dotąd naturalnie rozdzielana przestrzeń służbowa – praca w biurze, na firmowym sprzęcie i w firmowej sieci – stała się również strefą osobistą, służącą do spraw prywatnych, w tym konsumenckich. Stąd też, ofiarami ataków, realizowanych przez cyberprzestępców, stały się nie tylko przedsiębiorstwa, ale i osoby prywatne, narażone głównie na wykorzystanie ich emocji i na dezinformację. Wiele z tych ataków, do których doszło w 2021 r., opartych było na socjotechnice – przestępcy bazując na ludzkiej ciekawości, ale też na lękach wywołanych pandemią, używali znanych dotąd metod oraz złośliwego oprogramowania, podszywając się pod źródła instytucji zaufania społecznego jak Światowa Organizacja Zdrowia (WHO), Państwowa Inspekcja Sanitarna czy nawet organizacje charytatywne, tym samym skłaniając użytkowników do klikania w złośliwe linki i pobierania załączników. Oczywiste słabości wielu firm w cyber-ochronie, które uwydatniły się w nowych warunkach pracy, okazały się podatnym gruntem do cyber-nadużyć. W 2021 r. Polacy, pracujący głównie zdalnie lub hybrydowo, w większym stopniu niż dotychczas obawiali się, iż mogą stać się ofiarami cyberprzestępstwa. Liczba polskich obywateli, którzy wyrażali takie obawy wzrosła do 41% (z 36% w 2020 r.) i była najwyższa od pięciu lat[2].

Zatem, zarówno przed biznesem, jak i administracją państwową, w 2021 r., kolejnym roku pandemicznym, stanęło ogromne wyzwanie przeprowadzenia zmiany we wdrożeniu i realizacji procedur oraz usług bezpieczeństwa dla danych, urządzeń końcowych oraz samych pracowników. W dodatku, w terminie dotąd nie spotykanym. Dlatego, nie tylko cena za dostarczane usługi była najwyższym kryterium wyboru. Walutą było także wiarygodność i zaufanie. I także o tym jest poniższy Raport. Poza aktualizacją danych i informacji dotyczących omawianego okresu w kontekście cyberbezpieczeństwa, a także dalszymi rekomendacjami działań nie tylko dla branży cyfrowej, dokument porusza dotąd często pomijane aspekty. Należy bowiem pamiętać, że to właśnie firmy członkowskie, zrzeszone w Związku Cyfrowa Polska – liderzy najbardziej zaawansowanych technologicznie rozwiązań – zapewniali swoim klientom i partnerom biznesowym, to co trudno ująć w prostym podsumowaniu pandemicznego okresu: poczucie bezpieczeństwa opartego na wzajemnym zaufaniu.

1. „Barometr cyberbezpieczeństwa", KPMG, marzec 2021
2. Badanie CBOS, marzec 2021 r.

2. Skala cyberzagrożeń

2.1. Świat

Liczba użytkowników nowych technologii podłączonych do internetu systematycznie rośnie, ale to właśnie w czasie pandemicznych dwóch lat (2020 i 2021 r.) wzrosty były najbardziej spektakularne. W ciągu ostatnich dwóch lat tylko liczba użytkowników internetu na całym świecie zwiększyła się o 17%. Warto przy tym podkreślić, że z 4,1 mld w 2019 roku do aż 4,9 mld w 2021 r., wzrosła liczba osób, która choć raz korzystała z sieci internetowej[3]. Jednocześnie 5,22 miliarda ludzi na świecie korzysta już z telefonu komórkowego, a liczba unikalnych użytkowników mobilnych wzrosła w 2021 r. w porównaniu do roku poprzedniego o 1,8%. (do 93 milionów), a łączna liczba połączeń mobilnych zwiększyła się o 72 miliony (0,9%), osiągając łącznie 8,02 miliarda. Ponadto, ponad połowa całej światowej populacji korzysta obecnie z mediów społecznościowych, a średni dzienny czas korzystania z internetu na jednego użytkownika wynosi dziś 6 godz. 54 min[4]. Według najnowszych branżowych prognoz, za trzy lata na świecie działać będzie 38,6 miliarda, a 5 lat później - 50 miliardów urządzeń podłączonych do sieci internetowej[5].

Każda z tych liczb równa się liczbie potencjalnych ofiar cyberataku. Tym bardziej, że atakującymi nie są już tylko pojedyncze osoby, domorośli hakerzy, a raczej zorganizowane i wyspecjalizowane grupy przestępców.

Cybersecurity Ventures – ośrodek badawczy cyberprzestępczości – oszacował koszty w ten sposób generowane dla światowej gospodarki w 2021, na **6 bilionów dolarów amerykańskich, czyli 190 tysięcy dolarów amerykańskich na sekundę**. Dla porównania jeszcze 10 lat było to ok. 3 bln dol.

Tymczasem obecnie samych globalnych połączeń Internetu Rzeczy szacuje się na poziomie 8,6 miliarda, a do roku 2026 ich liczba ma wzrosnąć prawie trzykrotnie - do 23,6 miliarda! Ten wzrost oznacza więcej zagrożeń dla cyberbezpieczeństwa i luk w zabezpieczeniach, i co za tym idzie – wzrost wydatków na ich zabezpieczanie. Do 2026 r. mają one wynieść nawet 16,8 miliarda dolarów[6].

Urządzenia na świecie podłączone do sieci internetowej

2025
38,6 mld

2030
50 mld

To jak wielkim ryzykiem i zagrożeniem są ataki cybernetyczne, widać również w światowym rynku ubezpieczeniowym – w 2020 r. był wart 7 mld dolarów pod względem składki przypisanej brutto, a do 2025 r. jego wartość ma wzrosnąć do 20,6 mld USD, na co wpływ ma rosnące zagrożenie cyberatakami w wyniku pandemii[7].

16,8 **miliarda dolarów – tyle sięgną do 2026 r. wydatki na cyberbezpieczeństwo w skali globalnej**

3. Dane Międzynarodowego Związku Telekomunikacyjnego (ITU)
4. Raport: Digital Consumer Trends 2021 cz.2 | Deloitte
5. Prognozy Strategy Analytics
6. Raport ABI Research „Connected & protected: The vulnerabilities and opportunities of IoT security”
7. Global Data

2.2. Polska

A jak na tle tych danych wypada Polska? W styczniu 2021 r. w Polsce było 31,97 mln internautów, w tym, aż 25,90 mln użytkowników mediów społecznościowych. 98% Polaków używało telefonów komórkowych (w tym 97,6% smartfonów), 88,9% korzystało z laptopa lub komputera osobistego, 49,6% z tabletu, a 9,4% z inteligentnych urządzeń domowych[8]. Ponadto prawie dwie trzecie Polaków loguje się na co dzień do bankowości internetowej, a 55% do bankowości mobilnej. Co dziesiąty zarządza swoim kontem i zleca transakcje wyłącznie na telefonie komórkowym. Klienci banków coraz chętniej sięgają po usługi pozabankowe – 36% potwierdza, że za pomocą aplikacji bankowej działającej w smartfonie, jest dziś bardziej skłonna kupić ubezpieczenie, bilet komunikacji, a także opłacić miejsce parkingowe. Blisko co drugi Polak przyznaje, że w ostatnim roku realizował przez konto internetowe wiele spraw urzędowych, m.in. złożył wniosek w ramach programów Rodzina 500+, Dobry Start 300+ lub Czyste Powietrze[9].

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

Jeśli chodzi o polskie przedsiębiorstwa, to w przypadku ponad połowy z nich koronawirus spowodował wzrost inicjatyw związanych z cyfryzacją. Zdecydowana większość organizacji wdrożyła pracę zdalną, z wykorzystaniem służbowych laptopów i szyfrowanych połączeń (VPN). Jednocześnie ponad połowa polskich firm stwierdziła wzrost podatności na cyberataki w związku z wymuszonymi przez pandemię zmianami organizacji pracy. Co jedna ważne aż **64% z nich zanotowało w 2021 roku co najmniej jeden incydent dotyczący cyberbezpieczeństwa**. To wzrost o 10 punktów procentowych w porównaniu do roku 2019. Największe obawy dotyczą: wycieku danych z powodu złośliwego oprogramowania, wyłudzania haseł i innych danych uwierzytelniających oraz utraty nośników lub urządzeń mobilnych z danymi. Prawie co piąta firma zaobserwowała w zeszłym roku wzrost liczby cyberataków. Aż 58% firm uważa, że pandemia COVID-19 spowodowała wzmożone ryzyko ataków w sieci, jednak na zwiększenie budżetu finansującego cyberbezpieczeństwo zdecydowało się tylko 23% firm[10].

64% **firm w Polsce zanotowało w 2021 r. co najmniej jeden incydent dotyczący cyberbezpieczeństwa**

Także CERT Polska, zespół, który został powołany do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci, odnotował wzrost liczby obsłużonych incydentów. Najpopularniejszym z nich w okresie pandemicznego 2020 r. był phishing, czyli próba wyłudzenia danych — stanowił aż 73,15% wszystkich obsłużonych incydentów[11]. Ta forma cyberataku wystąpiła w 29% polskich firm[12].

8. Digital 2021 October Global Statshot Report - Digital in Poland 2021
9. Badanie na zlecenie Alior Banku
10. „Barometr cyberbezpieczeństwa 2021" KPMG, marzec 2021
11. Raport roczny CERT Polska - 2020 r.
12. Badanie Computerworld "Raport #CMIP 2021"

3. Świadomość nadużyć

Zdaniem ekspertów zajmujących się cyberbezpieczeństwem, choć wiedza dotycząca ochrony przed tego rodzaju zagrożeniami jest coraz większa, to nadal pozostaje do uzupełnienia, czasem nawet na fundamentalnym poziomie. W przypadku polskich konsumentów, prawie trzy czwarte z nich ma świadomość wykorzystywania ich prywatnych danych, a tylko co dziesiąty wie, jak nie dać się śledzić w Internecie. 73% Polaków uważa, że w internecie wykorzystywane są ich dane osobowe, a jednocześnie zaledwie 9% z nich ma świadomość istnienia narzędzi, które mogą temu zapobiec[13].

Jeśli chodzi o biznes to aż 55% dużych firm na świecie, nie powstrzymuje skutecznie cyberataków, nie potrafi ich zidentyfikować i szybko usunąć powodowanych przez nie naruszeń, a także ograniczyć ich negatywnych skutków. Liczba incydentów – obejmujących nieautoryzowany dostęp do danych, aplikacji, usług, sieci lub urządzeń – wzrosła rok do roku o 31%, średnio do 270 na firmę[14]. W polskich firmach, jedynie 41% firm bada wpływ potencjalnych cyberincydentów na funkcjonowanie przedsiębiorstwa, a 53% realizuje analizy ryzyka związane z ciągłością działania. Jednocześnie prawie wszystkie przedsiębiorstwa wdrożyły polityki związane z RODO. Pokazuje to, że wymogi regulacyjne stanowią wciąż kluczowy impuls stymulujący przedsiębiorców do działania w zakresie procedur związanych z cyberbezpieczeństwem[15].

Niestety, wciąż najsłabszym elementem w zakresie cyberochrony są pracownicy – żadna procedura nie będzie w tym zakresie skuteczna, jeżeli zespół nie będzie świadomy wymaganych od niego konkretnych działań i środków ostrożności. Z raportu Związku Firm Ochrony Danych Osobowych wynika, że 8 razy częściej powodem wycieku danych jest pojedynczy człowiek, niż technologiczne zapory i ochrona danych.

Istotnym zatem wydają się inwestycje nie tylko w rozwiązania bezpieczeństwa systemu IT, ale również w kompetencje pracowników, tworząc kulturę bezpieczeństwa i odpowiedzialności za aktywność w sieci. Choć w 2020 r. odsetek przedsiębiorstw stosujących środki bezpieczeństwa ICT wyniósł 95 %, tj. o 8,0 pkt. % więcej niż w roku poprzednim[16], to nadal służbowy sprzęt jest często używany do celów prywatnych – na smartfonach czy laptopach korzysta się z prywatnej skrzynki mail, instalowane jest oprogramowanie, oraz prowadzony stream filmów, programów TV czy podcastów.

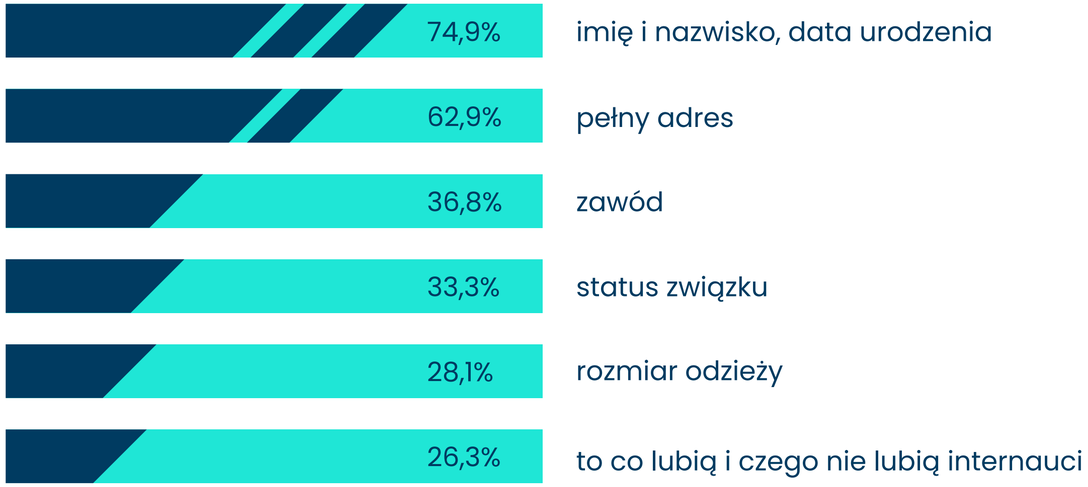
55 % **dużych firm na świecie, nie powstrzymuje skutecznie cyberataków, nie potrafi ich zidentyfikować i szybko usunąć powodowanych przez nie naruszeń, a także ograniczyć ich negatywnych skutków.**

13. Raport Deloitte "Digital Consumer Trends 2021"
14. Raport "State of Cyber Resilience 2021" Accenture
15. Badanie Computerworld "Raport #CMIP 2021"
16. Główny Urząd Statystyczny „Społeczeństwo informacyjne w Polsce w 2020 r".

4. Inne oblicze bezpieczeństwa

Trudno dziś sobie wyobrazić jakąkolwiek branżę czy obszar życia społecznego funkcjonujący w mniejszym, czy w większym zakresie, poza wirtualną rzeczywistością. Już nie tylko biznes i gospodarka, ale i zdrowie, kultura, a nawet relacje międzyludzkie ulegają rozwojowi technologii cyfrowych. To dzięki nim, powstaje ogromny i zarazem bezcenny zasób wiedzy i danych, do którego nieupoważniony dostęp może skutkować nie tylko naruszeniem prywatności, zakłóceniu w prowadzeniu działalności czy utratą własności intelektualnej, ale może być realnym zagrożeniem dla bezpieczeństwa państwa. Nowe badanie przeprowadzone przez dostawcę wirtualnych sieci prywatnych NordVPN ujawniło, że co trzeci Polak nie wyobraża sobie dnia bez internetu lub polega na internecie, a taka zależność zmusza go do dzielenia się wieloma poufnymi informacjami. Do najczęściej ujawnianych publicznie danych należą: imię i nazwisko, data urodzenia, pełny adres, zawód, status związku, a także rozmiar odzieży oraz to, co lubią i to, czego nie lubią internauci. Dodatkowo, co czwarta osoba z Polski publicznie ujawniła swój numer PESEL oraz dane konta bankowego.

Najczęściej ujawniane dane przez polskich użytkowników Internetu:



*Źródło danych: Badanie NordVPN

Trudno nie przekładać powyższych zachowań konsumenckich, na obawy dotyczące ochrony danych i informacji, na których oparta jest nie tylko cyfrowa gospodarka. Stąd, dla zapewnienia cyberbezpieczeństwa, powstały nowe rozwiązania, które nie sprowadzają się do jednego działania czy usługi, lecz holistycznie odnoszą się do zarządzania przedsiębiorstwem – jego produktami, usługami, pracownikami, procesami, etyką i wartościami, systemami, dostawcami i podwykonawcami. Przykładem takiego podejścia jest New Trust Standard firmy Cisco. Są to wytyczne dotyczące oczekiwań i odpowiedzialności, w ramach których firmy i ich klienci mogą określać nowe zasady rządzące relacjami opartymi na zaufaniu. To zbiór prostych zasadach, **a pierwsza z nich wynika z … braku zaufania**.

Traktuje ona wszystkie zasoby tak, jakby były zewnętrzne. Weryfikuje zaufanie do nich przed każdą próbą uzyskania dostępu. I zezwala na niego wyłącznie temu zasobowi, który jest wymagany. Jednak przede wszystkim, wprowadza kulturę przestrzegania tych samych praktyk i polityk w zakresie zabezpieczeń, przez klientów i partnerów biznesowych. Kolejne zasady to:

- **Zarządzanie ryzykiem generowanym przez dostawców i budowa zaufanego łańcucha dostaw**, choćby poprzez wymóg oprogramowania i sprzętu dokumentacji określającej pochodzenie ich produktów, czy regularnych audytów pod kątem słabym punktów.
- **Poszanowanie praw dotyczących danych**, które ma na celu umocnić zarówno prawa ich właścicieli, jak i narodową suwerenność, w oparciu nie tylko o przepisy prawne, ale również o technologię. Zaawansowane szyfrowanie, obliczanie poufne, zaciemnianie kodu i inne nowo powstające technologie i metody zwiększające prywatność oferują możliwość stworzenia modelu cyfrowej suwerenności w ramach bezpiecznego, otwartego i tętniącego życiem internetu.
- **Transparentność na temat prowadzonych działań**, to inaczej mówiąc szczerość i otwartość na temat tego, jak obchodzimy się z treściami klientów i co robimy z informacjami objętymi zasadami prywatności. Transparentna firma podejmuje odpowiednie działania, by chronić dane klientów i szanować ich prywatność. Dodatkowo, jest gotowa upubliczniać polityki, procesy i technologie, jakich używa w celu zabezpieczenia danych.
- **Regularne audyty i certyfikaty** to dowód dla klientów, organów regulacyjnych i innych interesariuszy, że sprzedawca przestrzega uznawanych na arenie międzynarodowej zasad prywatności, oraz że w odniesieniu do informacji umożliwiających identyfikację szanuje główne prawa tych, których dane te dotyczą. Nieustanna ewolucja usług w chmurze to także ewolucja kontroli bezpieczeństwa. Coroczna certyfikacja zapewnia stały sposób oceny profilu bezpieczeństwa sprzedawcy i ułatwia klientom podejmowanie świadomych decyzji.

5. Bezpieczne usługi i produkty w zasięgu ręki konsumenta

Wymuszona przez pandemię i związany z nią lockdown, przyspieszona cyfryzacja społeczeństwa, na stałe wprowadziła do wirtualnej przestrzeni obszary, które do tej pory były w niej obecne w sposób nieznaczny. Już nie tylko zakupy, ale także usługi finansowe,medyczne czy realizacja zadań biznesowych, są w zasięgu każdego konsumenta, bez potrzeby wychodzenia z domu. To wiąże się z koniecznością wyboru przez niego urządzenia końcowego tzw. end-to-end, zapewniającego poczucie bezpieczeństwa, pod kątem niezawodności, poufności i szybkości. Część procesów do jakich tego typu sprzęt jest używany, wymaga zarówno wykorzystania cyfrowej tożsamości użytkownika, jak i mechanizmów potwierdzenia woli, czyli zdalnej akceptacji czynności, którą użytkownik chce wykonać. Na przykład, niektóre oficjalne dokumenty, choć mogą być dostarczone online, wymagają istotnego szczegółu – podpisu lub innej formy dowodu niepodważalnie potwierdzającego tożsamość osoby składającej oświadczenie woli.

Rozwiązania, oparte o Usługi Zaufania umożliwiają bezpieczne zawieranie transakcji elektronicznych, w ramach określonych ram regulacyjnych, które mogą odbywać się między: konsumentami, podmiotami gospodarczymi czy administracją publiczną. Dzięki wykorzystaniu usług zaufania możliwe jest przeniesienie wielu czynności na poziom cyfrowy przy zachowaniu ważnych procedur i standardów. Usługi te są świadczone przez kwalifikowanych dostawców, którzy muszą spełniać wymogi wskazane w unijnym Rozporządzeniu eIDAS (Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE). Rejestr dostawców dostępny jest na stronie Narodowego Centrum Certyfikacji.

W katalogu Usług Zaufania wyróżnimy głównie:

- **Kwalifikowany podpis elektroniczny** - ma taką samą moc prawną jak unikatowy, własnoręczny podpis. Dokument cyfrowy, podpisany kwalifikowanym podpisem elektronicznym posiada więcej zalet niż dokument papierowy, podpisany odręcznie, ponieważ daje on pewność, iż w treść dokumentu nikt nie ingerował. Podobnie jak podpis własnoręczny, podpis elektroniczny jest jedyny w swoim rodzaju, ściśle powiązany z podpisywaną treścią i przypisany do konkretnej osoby fizycznej, która ten podpis złożyła. Sprawdzenie (weryfikację) autentyczności podpisu elektronicznego, w tym wiarygodne źródło identyfikacji tożsamości osoby podpisującej, zapewnia certyfikat, stanowiąc w powiązaniu z podpisem wirtualny dowód tożsamości użytkownika w sieci.

  - Podpis kwalifikowany zapewnia niezaprzeczalność oświadczenia woli wynikającej z podpisanej treści, gwarantując jednocześnie, że treść dokumentu nie została zmieniona w trakcie transmisji danych, w okresie przechowywania lub w wyniku celowej manipulacji.

  - Można dzięki niemu realizować prawnie wiążące transakcje na odległość, co Umożliwiają zapisy rozporządzenia eIDAS, uznawane we wszystkich krajach Unii Europejskiej.

Synergia bezpiecznego urządzenia mobilnego, jakim może być telefon, tablet lub laptop, z równie bezpiecznym e-podpisem, to właśnie przykład rozwiązania end-to-end. Dla konsumenta i użytkownika Internetu może on stanowić oczekiwaną wartość dodaną, adresującą z jednej strony jego potrzeby, a z drugiej, bezpieczeństwo w cyberprzestrzeni, zgodnie z zasadą: maksimum bezpieczeństwa przy utrzymaniu maksimum prywatności i prostoty działania.

- **Kwalifikowana pieczęć elektroniczna** - jest cyfrowym odpowiednikiem 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. Dokumenty opatrzone taką pieczęcią są wiążące w zakresie określonym w przepisach prawa i potwierdzają nadawcę dokumentu, dzięki procesowi weryfikacji podmiotu dokonywanego w procesie wydania certyfikatu przez jednostkę do tego upoważnioną.

- **Kwalifikowany znacznik czasu** – zapewnia bezpieczeństwo elektronicznych dokumentów poprzez powiązanie ich z konkretnym czasem (data pewna). Pozwala zabezpieczyć dokumenty przed sfałszowaniem i antydatowaniem

- **Kwalifikowana usługa walidacji** - jest to usługa, która wydaje poświadczenie potwierdzające autentyczność podpisu elektronicznego i pieczęci elektronicznej na podpisanym (podstemplowanym) dokumencie cyfrowym, stanowiąc gwarancję, że dokument nie został sfałszowany

- **Kwalifikowana konserwacja** – zapewnia przedłużenie technicznych i prawnych możliwości weryfikacji podpisu elektronicznego i pieczęci elektronicznej, tym samym zapewniając ich wartość dowodową (prawną) w długim okresie

Wykorzystanie w praktyce powyższych narzędzi, umożliwiły między innymi **zdalną obsługę klienta**, a tym samym zachowanie ciągłości biznesowej sprawne funkcjonowanie firmy z zachowaniem wszelkich środków bezpieczeństwa, wymuszonych przez pandemię.

Przykłady:

- Możliwość zdalnego podpisywania umowy rezerwacyjnej na zakup nieruchomości bez konieczności fizycznego spotkania z przedstawicielem dewelopera, a co za tym idzie, podpisania umowy papierowej. Rezultatem wdrożenia usług cyfrowych była gwarancja rezerwacji mieszkania, podniesienie wiarygodności umowy, dzięki zastosowaniu podpisu elektronicznego, zachowanie ciągłości biznesowej, która w okresie pandemii i lock-downu była zagrożona.

- Zawieranie umów z klientem bez konieczności podpisywania dokumentów w formie papierowej, dzięki **zastosowaniu urządzenia mobilnego, który można poddać dezynfekcji oraz podpisu biometrycznego (rysikiem na tablecie).**

- Zastosowanie **platformy do e-podpisu**, umożliwiającej elektroniczne podpisywanie wszystkich dokumentów, niezależnie od urządzenia, z którego użytkownik korzysta. Pozwoliło to przedsiębiorstwu na podtrzymanie działań operacyjnych podczas pandemii.

- Istotnym elementem transformacji procesów biznesowych jest także wprowadzenie rozwiązań, które pozwolą na zdalną Identyfikację osób - takich jak zdalne potwierdzenie tożsamości wykorzystujące kanały audio i video.

6. Podsumowanie

Choć organizacje - zarówno te w sektorze prywatnym, jak i państwowym, na bieżąco wprowadzają procedury związane z cyberbezpieczeństwem oraz zarządzaniem ryzykiem informatycznym, to nieustannych inwestycji wymaga obszar związany z ochroną urządzeń końcowych: smartfonów, tabletów, laptopów, komputerów stacjonarnych, drukarek i urządzeń wielofunkcyjnych. Wydaje się to być nie do uniknięcia w obliczu przestawienia się gospodarek na tory pracy zdalnej i hybrydowej.

Żadna organizacja czy instytucja nie jest wolna od cyberprzestępczości, szczególnie gdy posiada kontakty międzynarodowe. **Zatem jednym z najwyższych priorytetów jest kwestia edukacji** - zarówno społecznej, jak i organizacyjnej, w tym administracji publicznej czy MŚP (mały i średni biznes) – która zwiększy świadomość wszystkich użytkowników na temat ochrony przed cyberzagrożeniami. Zarówno w przypadku małego i średniego biznesu, a także instytucji publicznych cyberbezpieczeństwo powinno być uwzględniane w każdym wymiarze ich funkcjonowania - od planowania, zakupów i inwestycji, po produkcję, i obsługę klienta. Za każdym z tych działań stoi człowiek, a jak wskazaliśmy w powyższym Raporcie, to właśnie człowiek jest najsłabszym ogniwem w procesie zapewniania ochrony danych którymi dysponuje, jako właściciel firmy, pracownik czy po prostu konsument. Dlatego, na podstawie dotychczasowych doświadczeń firm technologicznych, tworzących Związek Cyfrowa Polska, przygotowaliśmy rekomendacje dotyczące ochrony urządzeń końcowych i zawarliśmy je w dalszej części dokumentu.

Kolejnym, równie ważnym zadaniem zarówno dla sektora prywatnego, jak i państwowego, jest ścisła współpraca na rzecz cyberbezpieczeństwa państwa. Owocem takiej współpracy są choćby przedstawione w ostatnim czasie przez Urząd Zamówień Publicznych, rekomendacje dotyczące zamówień publicznych na systemy informatyczne, które powstały przy udziale ekspertów Związku Cyfrowa Polska. Dzięki temu, powstał szeroki zestaw praktycznych porad, niezbędnych do przeprowadzenia postępowania o udzielenie zamówienia publicznego na systemy IT, na każdym jego etapie - od sformułowania Opisu Przedmiotu Zamówienia, po kryteria cenowe i pozacenowe, w tym szczególnie kwestii cyberbezpieczeństwa, która niestety wciąż bywa w tych procesach zaniedbywana. **Świadomość cyberzagrożeń i zrozumienie idących za nimi konsekwencji, jest kluczowym elementem w przetargowych postępowaniach administracyjnych.**

Wśród dalszych promowanych przez Związek Cyfrowa Polska działań na rzecz unormowania i zachowywania szeroko rozumianego cyberbezpieczeństwa są **propozycje uruchomienia programu „bonów na cyberbezpieczeństwo”.** To pomysł na fundusze publiczne dostępne dla jednostek samorządowych na zakup usług lub rozwiązań z zakresu bezpieczeństwa, przygotowanych dla nich przez polskie firmy lub jednostki badawcze. Z kolei dla sektora małych i średnich przedsiębiorstw - Związek proponuje by **kwalifikować wydatki na cyberbezpieczeństwo jako wydatki na innowacje, czyli rozszerzyć ulgę na innowacyjność w zakresie zakupu narzędzi do zachowania cyberbezpieczeństwa.**

Ale nie tylko szeroko rozumiana edukacja i współpraca na polu administracja – biznes, będzie miała wpływ na powodzenie procesu cyfrowej transformacji, wymuszonej na globalnym gospodarczym organizmie przez pandemię. To także dostęp do innowacji wypracowanych w oparciu o najnowsze technologie, oferowane przez liderów branży technologicznej, w tym zrzeszonych w Związku Cyfrowa Polska. Dzięki nim, **realnym się staje podjęcie wyzwań z jakimi mierzy się polskie społeczeństwo i polska gospodarka.**

7. Rekomendacje

7.1. Rozwiązania poprawiające bezpieczeństwo urządzeń mobilnych

- **Platformy bezpieczeństwa oparte na oddzielnym podsystemie sprzętowym:**
  To dedykowane moduły z własną pamięcią i proceroserm które w oddzielnym, odizolowanym od głównego systemu operacyjnego magazynie, przechowuje wrażliwe dane, takie jak hasła, dane biometryczne czy też klucze kryptograficzne. 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 hybry-dowym środowisku chmurowym. Pełna integracja z urządzeniami typu tablet czy smartfon, z dostępnymi usługami dostawcy, zapewnia kompleksowe dostosowanie do konkretnych potrzeb, tym samym przekształcając je 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 prostemu, nieskomplikowanemu UX, administratorzy IT mogą zmaksymalizować produktywność, poprzez zdalne śledzenie, zarządzanie, rozwiązywanie problemów, konfigurowanie i wysyłanie wiadomości do urządzeń. Umożliwiają zarządzanie dowolnym urządzeniem z najbardziej popularnymi systemami: Android, iOS.

- **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 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, oprogramowanie 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.

- **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

7.2. Certyfikacja 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, rygorystyczne niezależne testy funkcjonalności oraz analizę luk w zabezpieczeniach 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.

7.3. Ochrona drukarek i urządzeń wielofunkcyjnych przed cyberzagrożeniami

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 pendrivów, jak również bezpośrednich wydruków z komputera),
- umożliwiają definiowania 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, aniżeli 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.

7.4. Ochrona laptopów i komputerów stacjonarnych przed cyberzagrożeniami

Laptop i komputer stacjonarny powinny posiadać:

- Dysk z funkcją samoszyfrowania SED (self-encyption drive) zgodny ze standardem OPAL2.
- W przypadku laptopów i notebooków wbudowana dodatkowa kamera podczerwieni (Infra Red) pozwalająca 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.