

Jak bezpiecznie prowadzić firmę?

Poradnik dla przedsiębiorców
część II



Spis treści

Wstęp.....	3
Bezpieczna firma, czyli jaka?.....	4
Uwaga, awaria.....	6
Cyberbezpieczeństwo w małej firmie.....	10
Jak zabezpieczyć komputer i dane?.....	16
Wsparcie IT.....	20
Bezpieczne dane i dokumenty.....	24



Bezpieczeństwo w małym biurze

Polscy przedsiębiorcy są świadomi czyhających na nich zagrożeń i wciąż szukają sposobów na poprawienie bezpieczeństwa w firmie. Przeciwno sobie mają jednak nie tylko cyberprzestępców, lecz także zwykłą ludzką nieuwagę i nieprzewidziane zdarzenia.

W poradniku podpowiadamy, jak dbać o sprzęt komputerowy, by zabezpieczyć się przed przykrymi i kosztownymi niespodziankami.



Bezpieczna firma, czyli jaka?

Na bezpieczeństwo firmy, w której działalności ważne miejsce zajmuje komputer i przechowywane w nim dane, składa się kilka czynników. Choć najczęściej mówi się o odpowiednim zabezpieczeniu sprzętu, praca zaczyna się znacznie wcześniej.

Co może zaburzyć jej płynność?

- Mechaniczne awarie sprzętu.
- Utrata danych lub dokumentów.
- Problemy z konfiguracją urządzeń.
- Nieznajomość niektórych funkcji obsługiwanych programów i aplikacji.
- Cyberataki, w tym przejęcie firmowych danych, żądanie okupu za przywrócenie dostępu do komputera czy przejęcie firmowego konta w mediach społecznościowych.

Dlatego równie ważna jak **ochrona przed cyfrowymi oszustami jest dbałość o **odpowiednią archiwizację i wsparcie IT.****



Cyfrowe Biuro Orange – rozwój bez zbędnych niespodzianek

Poznaj najczęstsze problemy, z jakimi borykają się właściciele firm, oraz proste sposoby na rozwiązanie każdego z nich.

Wsparcie IT:



Awarie komputerów – szczególnie matryc oraz dysków – ich samodzielna wymiana grozi uszkodzeniem innych elementów komputera.



Błędy konfiguracji i działania systemu operacyjnego – niekiedy jedno niewłaściwe kliknięcie potrafi unieruchomić komputer... i biznes.



Awarie „wtyczek” przeglądarek internetowych – potrafią skutecznie utrudnić korzystanie z internetu.



Problemy z konfiguracją i przestojami drukarek – zdarzają się, gdy trzeba na szybko wydrukować umowę lub dokumenty do urzędu.



Problemy z konfiguracją spotkań telekonferencyjnych – wybór właściwej kamery czy odblokowanie dostępu do sieci firmowej.

Microsoft 365:



Nagle L4 pracownika lub inna przyczyna, przez którą nie mamy dostępu do jego danych.



Brak prądu w biurze lub inna awaria – jak pracować, gdy nie mamy pełnego dostępu do biura? Rozwiązanie poniżej!

CERT Orange Polska:



Fałszywe linki – prowadzą do stron wyludzających dane. Dla przedsiębiorców najbardziej ryzykowne są fałszywe strony bankowości internetowej.



Wirusy, trojany, robaki – mogą doprowadzić do kradzieży danych i blokady komputera w celu wymuszenia okupu.

Zestawienie najczęstszych problemów technicznych przygotowaliśmy razem z klientami.

Uwaga, awaria

Problemy ze sprzętem zawsze wiążą się ze stresem, a koszty naprawy potrafią nadszarpnąć finanse firmy. Co gorsza, mogą powodować przestoje w pracy lub doprowadzić do utraty cennych danych, a co za tym idzie – utraty reputacji i wielu szans biznesowych.



Najczęściej spotykane usterki

Przeważnie komputery trafiają do serwisów z kilku powtarzających się powodów.

Oto najczęściej spotykane usterki:



Konieczność wymiany dysku



Uszkodzona matryca



Zalanie urządzenia



Wyłamane gniazdo i obudowa wiatraka

Dobra wiadomość jest taka, że części z nich można uniknąć, odpowiednio dbając o sprzęt.



Ekspert radzi:

Jakie straty może ponieść mała firma z powodu awarii sprzętu komputerowego?

„Niesprawne komputery wpływają na efektywność firmy na każdym polu i mogą prowadzić do obniżenia jakości obsługi. Na przykład księgowej: utrata danych wskutek awarii komputera wiąże się z koniecznością ich ponownego wprowadzenia i opóźnieniami. W przypadku działalności tak silnie uzależnionej od terminowości jak usługi księgowe oznacza to często **pogorszenie reputacji lub nawet utratę klientów**.

Potwierdzają to liczby: **blisko jedna czwarta klientów, których doświadczenie ze współpracy z firmami było złe, zmniejszyła swoje wydatki u nich, zaś jeden na pięciu całkowicie zrezygnował ze współpracy** – potwierdza to badanie przeprowadzone przez Qualtrics XM Institute.

Dlatego każdej firmie przyda się kompleksowy plan działania na wypadek problemów ze sprzętem: możliwość uzyskania szybkiej pomocy technicznej, dostęp do zastępczego komputera czy opcja odtworzenia utraconych danych mogą dosłownie uratować biznes”.

” **Niesprawne komputery wpływają na efektywność firmy**



Jakub Olechowski
Senior Solutions Manager
Rozwiązania ICT

Lepiej zapobiegać, niż leczyć

Myśl o kosztach naprawy laptopa i problemach, jakie może spowodować zepsucie się sprzętu w najmniej odpowiednim momencie, powinna stanowić dobrą motywację do pracy nad nową komputerową rutyną w firmie.

Choć wśród najczęstszych przyczyn awarii sprzętu wciąż są zalania, zabrudzenia czy niewłaściwy transport, prawdopodobieństwo wystąpienia tych problemów da się zminimalizować, stosując kilka prostych zasad. O zasadach tych opowiemy Ci na kolejnej stronie.

Komputerowe BHP, czyli jak dbać o komputer, by nie bać się awarii

Najlepszy środek na zdrowe zawiasy

W trosce o zawiasy i matrycę zamykaj i otwieraj swojego laptopa delikatnie, trzymając za środek matrycy, a nie po bokach.

Zamknięty laptop to bezpieczny laptop

Zawsze lepiej przemieszczać się z zamkniętym laptopem, trzymając go oburącz od spodu. Otwarta matryca utrudnia uchwyt i grozi upuszczeniem urządzenia lub uszkodzeniem zawiasów.

Co wygodne dla nas, niekoniecznie dla laptopa

Praca z laptopem na kolanach, w łóżku czy na kocu zatyka otwory wentylacyjne i uniemożliwia prawidłowe chłodzenie urządzenia.

Kawa, herbata, woda? Poniżej laptopa

Lepiej pracuje Ci się z wodą zawsze pod ręką? To zdrowe, ale by było też zdrowe dla Twojego laptopa, trzymaj ją poniżej poziomu laptopa, np. na stoliku obok biurka.

Wyższy poziom bezpieczeństwa? W pionie

Bezpieczniej przewozić laptopa w pionie – jest wtedy mniej narażony na drgania.

Proste jak... kabel

Powyginane i naprężone kable od ładowarki i innych urządzeń mają nie tylko skróconą żywotność, ale tworzą też naprężenia niebezpieczne dla gniazd, szczególnie ładowania.

Bezpieczny transport

Kobieca torebka lub wysłużony plecak potrafią zmieścić wszystko, ale Twój laptop będzie bezpieczniejszy w torbie lub plecaku z komorą amortyzującą wstrząsy i dopasowaną wielkością do jego matrycy.

Wyłączony na czas podróży

Aby uniknąć przegrzania i uszkodzeń, powinno się całkowicie wyłączyć komputer, a nie tylko wprowadzać w tryb uśpienia. Jeśli na dworze jest mróz, odczekaj trochę, nim ponownie włączysz komputer wewnętrzny.

Cyberbezpieczeństwo w małej firmie

Równie ważne jak ochrona sprzętu przed urazami mechanicznymi jest zapewnienie bezpieczeństwa w sieci. Właściciele małych i średnich firm zdają sobie sprawę z tego, że cyberataki stanowią realne zagrożenie.

Jedna na pięć firm doświadczyła cyberataków, a ponad połowa (58%) negatywnie ocenia poziom bezpieczeństwa IT – wynika z badania „Postawy wobec cyberzagrożeń w SOHO i SME”, przeprowadzonego przez KANTAR dla Orange.

Cyberprzestępcy wiedzą, że najsłabszym punktem zwykle jest człowiek – użytkownik, który w pośpiechu otworzy fałszywą wiadomość lub wejdzie na nieodpowiednią stronę.



Cyberataki – duży problem dla małych firm?

Aż **1 na 7** małych firm doświadczyła ataku w 2020 roku. Dziennie w Polsce dochodzi do **2 mln** cyberataków.

Oto najczęstsze rodzaje cyberataków:

-  **35%** Złośliwe oprogramowanie (PC)
-  **33%** E-maile/telefony od oszustów (phishing)
-  **27%** Brak dostępu do usług internetowych
-  **23%** Kradzież danych
-  **16%** Żądanie zapłaty w zamian za odzyskanie kontroli nad urządzeniem (ransomware)
-  **12%** Złośliwe oprogramowanie (smartfon)
-  **8%** Ataki DDoS na stronę WWW firmy

W jaki sposób małe firmy zabezpieczają się przed zagrożeniami?

Oto najczęstsze sposoby:

-  **89%** Programy antywirusowe
-  **89%** Login i hasło
-  **47%** Blokady ekranu
-  **41%** Przechowywanie danych w chmurze
-  **39%** Regularny backup danych
-  **23%** Szyfrowanie dysków

A man with a beard is working on a laptop in a workshop. Overlaid on the image is a network diagram with orange lines connecting various colored dots (yellow, blue, green, pink, purple).

Naucz się rozpoznawać fałszywe wiadomości

Jak rozpoznać fałszywe wiadomości?

Niezależnie od tego, jakimi sposobami cyberprzestępcy będą próbowali przejąć dane Twojej firmy, istnieje kilka uniwersalnych zasad, których przestrzeganie zauważalnie zwiększa bezpieczeństwo w sieci.

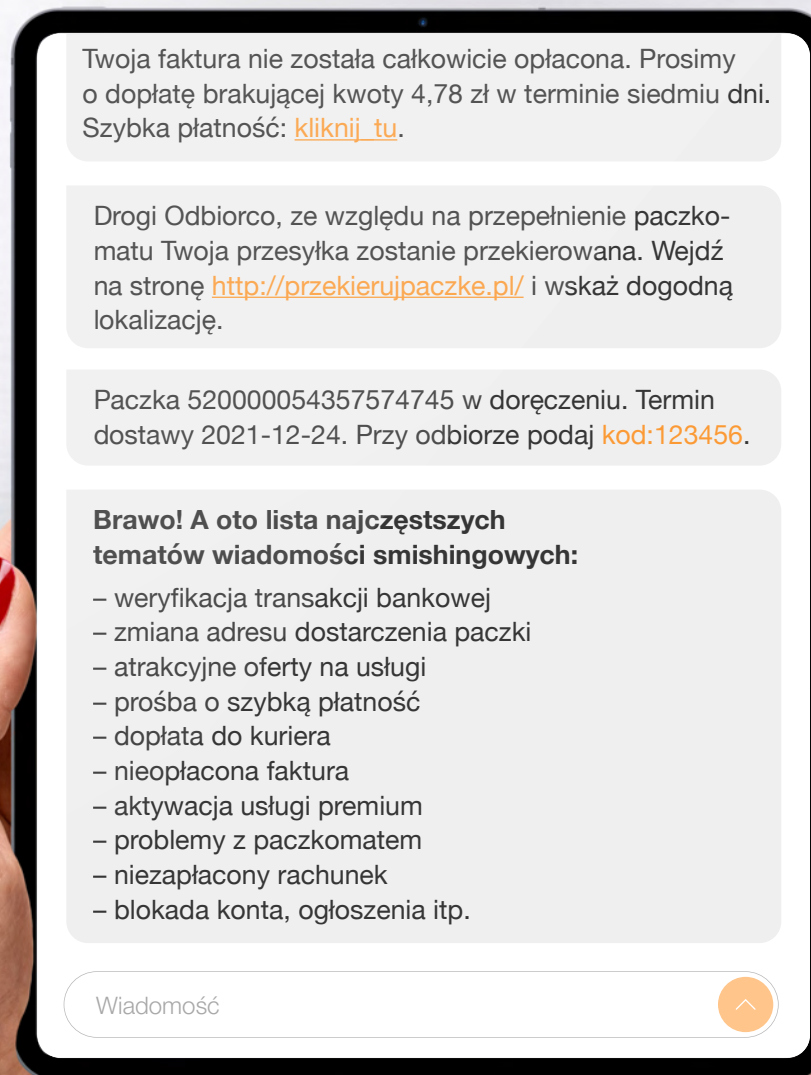
Twoją czujność powinny zawsze budzić następujące elementy:

- Niestandardowo wyglądające linki w wiadomości.
- Adres e-mail nadawcy, w którego domenie nie ma nazwy firmy.
- Wszelkie prośby o dopłaty.
- Nieznane lub źle zapisane nazwy firm kurierskich, banków i instytucji.
- Błędy, literówki i potoczny język w treści wiadomości.

Jeśli w wiadomości, którą otrzymasz, znajduje się przynajmniej jeden z tych elementów, to prawdopodobnie jest ona próbą oszustwa.

Smishingowe ABC, jak nie dać się nabrać na SMS od oszusta

Oto kilka przykładów smishingu i jedna prawdziwa wiadomość. Czy rozpoznasz, która nie jest próbą oszustwa?



Czego nigdy nie robić z fałszywą wiadomością?

W przypadku prób wyłudzenia danych ważniejsze od tego, co zrobisz, jest to, czego nie zrobisz.

Jeśli nie masz całkowitej pewności co do autentyczności maila lub SMS-a, nigdy:

- nie klikaj w link
- nie oddzwaniaj na numer w wiadomości
- nie odpisuj
- nie próbuj płacić żadnych pieniędzy
- nie podawaj nikomu kodów BLIK

Jeśli nadawcą podejrzanej wiadomości jest bank, firma kurierska lub instytucja, z którą współpracujesz, wyjaśnij sprawę, kontaktując się oficjalnymi kanałami (np. pod numerem telefonu podanym na oficjalnej stronie).

Pamiętaj, że podejrzone wiadomości mogą również wysłać osoby podszywające się pod Twoich znajomych i członków rodziny. Dlatego każdą prośbę bliskich o pieniądze lub pomoc w dokonaniu przelewu lepiej zweryfikować telefonicznie lub osobiście.



Czego nigdy nie robić z podejrzaną wiadomością

Ekspert radzi:

Jakie są największe cyberzagrożenia dla przedsiębiorców i jak się przed nimi skutecznie bronić?

„Jednym z najgroźniejszych ‘oręży’ cyberprzestępców jest socjotechnika. **Podszywanie się pod firmy i instytucje, takie jak kurierzy, banki czy dostawcy usług** (także telekomunikacyjnych), to sposób na przejęcie danych do bankowości elektronicznej, firmowych kart kredytowych czy dostępów do serwisów, z jakich korzysta przedsiębiorca – a tym samym nierzadko także danych jego klientów.

Kanały komunikacji, z których korzysta na co dzień przedsiębiorca, są atrakcyjnymi ‘bramkami’ dla ataków phishingowych. **Do najpopularniejszej formy, czyli e-maili, doszły SMS-y (smishing) oraz phishing głosowy (vishing).** I jak pokazują liczby, te metody niestety działają: aż **80%** odbiorców próbuje wejść na stronę phishingową w ciągu 15 minut od otrzymania SMS-a. To, na co powinniśmy również zwrócić szczególną uwagę, to tajemnicze faktury. Bardzo często kliknięcie w nie prowadzi do zainstalowania szkodliwego oprogramowania typu banker, wyspecjalizowanego w wykradaniu m.in. danych logowania do banków.

Podstawą ochrony jest oczywiście wzmożona czujność, którą najlepiej wzmocnić rozwiązaniami technologicznymi, takimi jak **CyberTarcza**. **Tylko w zeszłym roku zablokowała ona aż 40 milionów prób wejścia na strony phishingowe”.**

” Podstawą ochrony jest wzmożona czujność



Michał Rosiak
Ekspert CERT Orange Polska

Jak zabezpieczyć komputer i dane?

Przestrzegając zasad, zachowując ostrożność i stosując dobre praktyki, zdecydowanie zmniejszasz ryzyko ataku. Dodatkowo na rynku dostępnych jest wiele rozwiązań, które pomogą podnieść bezpieczeństwo w Twojej firmie.





Program antywirusowy czy CyberTarcza?

Jak pokazują cytowane wcześniej badania, zdecydowana większość firm (**89%**) korzysta z programów antywirusowych. To dobra praktyka, choć nie jedyna. Pamiętaj, że coraz więcej programów komputerowych ma również swoje wersje mobilne. Tymczasem według badań firmy Bellini **aż 71% Polaków nie zabezpiecza swoich smartfonów.**

Dla właścicieli firm, którzy szukają rozwiązań chroniących przed skutkami wrogiej aktywności zarówno w sieci stacjonarnej, jak i mobilnej, dobrym wyjściem może być **CyberTarcza** – autorskie rozwiązanie Orange Polska.

To mechanizm, który wykrywa zagrożenia płynące z internetu i blokuje je, zanim dotrą do komputera czy smartfona. W przeciwieństwie do tradycyjnych programów antywirusowych nie wymaga instalacji na urządzeniu. Dzięki temu nie spowalnia komputera czy smartfona. Działa szybciej i nie wymaga instalowania aktualizacji.

Co wybrać – antywirus czy CyberTarczę? Najlepiej stosować oba te rozwiązania jednocześnie.

Firewall (Orange Network Security, Zarządzany UTM)

Wszystkie firmy korzystające z internetu i posiadające własną infrastrukturę potrzebują profesjonalnego zabezpieczenia sieci. Jest to szczególnie ważne w czasach, gdy do firmowych danych mają dostęp osoby znajdujące się w różnych miejscach i korzystające z różnych urządzeń.

Inwestycja w profesjonalny sprzęt blokujący niebezpieczny ruch z sieci może przewyższać budżety mniejszych firm. Nie jest to jednak przeszkodą w przypadku usługi Orange – Zarządzany UTM, która dostępna jest w modelu abonamentowym. A dzięki połączeniu usług internetowych, VPN oraz usług z zakresu cyberbezpieczeństwa pozwala zoptymalizować koszty.

Usługa zapewnia całodobowy monitoring zainstalowanych w sieci urządzeń UTM. Specjaliści zarządzają konfiguracją urządzeń i zapewniają jej backup. Usuwane są również wszystkie awarie, szkodliwa zawartość z kodu HTML i inne nieprawidłowości.





Zabezpiecz PESEL, monitoruj NIP

Mając dostęp do numeru PESEL, przestępcy mogą założyć na Twoje dane firmę, wziąć kredyt lub podpisać umowę abonentową. Takie praktyki narażają reputację Twojej firmy i kosztują wiele nerwów. Czy da się temu zapobiec? Na szczęście tak!

Jednym ze sposobów jest usługa Zabezpiecz PESEL, z której mogą skorzystać klienci Orange zawierający lub przedłużający umowę na abonament komórkowy. Dzięki niej otrzymasz powiadomienia, ilekroć Twoje dane pojawią się w systemach najważniejszych instytucji i będziesz mógł w porę zareagować. Powstrzymasz też próbę oszustwa.

Dodatkowo możesz też monitorować numery NIP kontrahentów – także tych nowych, z którymi planujesz dopiero rozpocząć współpracę. Usługa Orange pozwala na sprawdzenie, czy firma widnieje w Krajowym Rejestrze Długów, a tym samym zweryfikowanie jej wiarygodności.

W ramach usługi monitorowanych jest 328 banków, 150 firm pożyczkowych oraz 15 firm telekomunikacyjnych. Dane są weryfikowane również na podstawie wpisów w Krajowym Rejestrze Długów oraz Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Wsparcie IT

Oprócz wdrażania dobrych praktyk korzystania z laptopa i bezpieczeństwa w sieci każdy przedsiębiorca potrzebuje czasem konsultacji ze specjalistą IT. Przejście wielu firm, urzędów i instytucji przynajmniej częściowo w tryb zdalny sprawiło, że konieczne stały się nowe modele wsparcia informatycznego.



Ekspert radzi:

Jakie czynności związane z obsługą komputera, a niekoniecznie awarią, lepiej powierzyć wsparciu IT, by uniknąć problemów?

„Blisko dwie trzecie (**65%**) małych firm korzysta z usług Over The Top, takich jak komunikatory internetowe czy videokonferencje – podaje Urząd Komunikacji Elektronicznej. Komputer stał się kluczowym narzędziem komunikacji, dlatego tak ważne jest jego niezawodne działanie.

Warto podkreślić, że nie trzeba awarii podzespołów laptopa, by skutecznie ‘wyłączyć go’ z funkcjonowania na rzecz firmy. **Niewłaściwie dokonana reinstalacja oprogramowania** może zakończyć się bardzo podobnie – w myśl zasady, że komputer jest tak dobry jak zainstalowane na nim oprogramowanie... i odwrotnie. Konsultacja ze specjalistą IT może nas również uchronić przed instalacją **złośliwego oprogramowania**.

Wielu przedsiębiorców ma **problemy z użytkowaniem niektórych funkcji programów biurowych**, np. tworzeniem formuł czy zestawień w arkuszach kalkulacyjnych programu Microsoft Excel. Pracujemy na bardzo wrażliwej materii, jaką są nasze firmowe dane, dlatego jeśli nie jesteśmy czegoś pewni – zadzwonimy do Wsparcia IT”.

” **Niesprawne komputery wpływają na efektywność firmy**



Paweł Jagóra
Senior Solutions Manager

Fachowa pomoc w codziennej pracy

Nie chodzi tylko o naprawy i pomoc w sytuacjach kryzysowych, lecz także o wsparcie w codziennej pracy na komputerze. Wyskakujące błędy o niewiele mówiących numerach i opisach mogą być źródłem frustracji. Co gorsza, zwykle skutkują opóźnieniami i błędami w pracy.

Oszczędność czasu

To, co informatyk zrozumie i naprawi w minutę, laikowi może zająć kilka wypełnionych nerwami godzin. Godzin, które mogą okazać się kluczowe dla funkcjonowania Twojego biznesu. Dlatego tak ważna jest szybka reakcja informatyka, ilekroć pojawią się problemy z firmowym sprzętem lub oprogramowaniem. Wiele z nich można wyeliminować zdalnie, podczas rozmowy telefonicznej lub udzielając zdalnego dostępu do pulpitu. Dzięki temu oszczędzasz czas, a odległość nie stanowi problemu.

Kilka faktów dotyczących naszej pomocy w ramach Wsparcia IT

Wiemy, że w prowadzeniu firmy ważna jest każda minuta. Zobacz, jak szybko Wsparcie IT może pomóc Ci w rozwiązywaniu problemów ze sprzętem komputerowym.

Oto najczęstsze rodzaje cyberataków:



15 minut Średni czas konsultacji telefonicznej



90% Spraw finalizowanych przy pierwszym kontakcie z infolinią



2 godziny Czas reakcji i diagnoza problemu



24 godziny Wizyta w firmie Klienta



24 godziny Udostępnienie sprzętu zastępczego

Jak Wsparcie IT najczęściej pomaga przedsiębiorcom?



Pomoc w odzyskaniu utraconych plików



Konfiguracja, aktualizacja i reinstalacja systemu i oprogramowania



Pomoc w obsłudze zaawansowanych funkcji programów biurowych



Konfiguracja firmowego internetu



Usuwanie awarii

Zapewnić wsparcie IT i nie zbankrutować

Usługi IT zwykle należą do kosztownych, a eksperci w tej dziedzinie wysoko wyceniają swój czas. Istnieją jednak rozwiązania dające dostęp do kompleksowych usług IT w ramach niewielkiej, stałej opłaty miesięcznej. Jednym z nich jest Wsparcie IT w Orange dla Firm. Płacąc od kilkunastu do kilkudziesięciu złotych miesięcznie, w zależności od wybranego pakietu, możesz zapewnić sobie stałą, kompleksową opiekę zespołu specjalistów.

Podstawowy pakiet obejmuje dostęp do infolinii, opiekę konsultanta i naprawę poprzez zdalne zalogowanie do komputera. Bardziej rozbudowane warianty przewidują również fizyczne obejrzenie sprzętu przez informatyka i zabranie laptopa do naprawy, a w razie potrzeby udostępnienie komputera zastępczego.



Bezpieczne dane i dokumenty

Przechowywanie firmowych dokumentów stało się o wiele prostsze, odkąd nie trzeba magazynować w szafach ton wydruków. Jednym kliknięciem można uzyskać dostęp do archiwów i wyszukać potrzebne pliki. Niestety czasami równie łatwo – jednym nieostrożnym kliknięciem – można je skasować.

Czy pamiętasz o tworzeniu kopii zapasowych?

Zrobienie kopii zapasowej nic nie kosztuje i trwa chwilę. Odzyskanie utraconych danych – wręcz przeciwnie. Pomimo tego przedsiębiorcy wciąż nie zawsze pamiętają o zapisywaniu na bieżąco ważnych plików.



Zrób kopie zapasowe i nie martw się na zapas

Dbłość o bezpieczeństwo danych i łatwy dostęp do nich jest bardzo ważna, ponieważ:



114 dokumentów musi rocznie przekazać urzędom przeciętna polska mikrofirma



Około **30 dni** trwa średnio proces fakturowania i płatności. W przypadku zagubienia dokumentów – potrafi znacznie się wydłużyć



Szacuje się, że **7,5%** dokumentów ginie w firmach bezpowrotnie – co może narazić firmę na straty finansowe i konsekwencje prawne



2/3 przypadków utraty wszystkich danych notuje się właśnie w firmach

Tymczasem:



Tylko **39%** firm SOHO robi regularny backup danych w komputerach



60% firm SME regularnie robi kopie zapasowe danych z komputerów



24% firm SOHO robi backup danych w smartfonach



38% SME zabezpiecza tak dane ze smartfonów

Źródło danych: Konfederacja Lewiatan; badanie „Can you trust your backups”



Automatyczna archiwizacja w Microsoft 365

Tworzenie backupów to jedna z tych rzeczy, które każdy uważa za pożyteczne, ale nie każdy stosuje w praktyce. Często jest to kwestią braku odpowiednich nawyków. Zamiast liczyć na zawodną ludzką pamięć, lepiej postawić na automatyczne rozwiązania. A takich dostarcza w tym zakresie Microsoft 365 w usłudze OneDrive.

Jak korzystać z usługi OneDrive?

Użytkownicy Microsoft 365 mają możliwość włączenia autozapisu w plikach, nad którymi pracują. Zmiany zapisują się wówczas automatycznie nie tylko na urządzeniu, lecz także w chmurze, w usłudze OneDrive.

Jeśli zajdzie potrzeba, dostęp do plików można także przydzielić kolejnym osobom oraz określić, czy mogą je edytować, czy tylko przeczytać.

Korzystanie z usługi OneDrive jest wyjątkowo proste. Wystarczy:

- Utworzyć konto Microsoft.
- Włączyć funkcję „Autozapis” w plikach pakietu Office (w lewym górnym rogu).
- Gotowe Twoje pliki automatycznie trafiają do chmury

Łatwe udostępnianie

Usługa OneDrive pozwala na udostępnianie plików współpracownikom i klientom. Wystarczy wysłać link w wiadomości e-mail lub SMS. Dzięki aplikacjom pakietu Office możesz również współdziałać w czasie rzeczywistym przy tworzeniu dokumentów. Tym samym jest to świetne narzędzie do efektywnej pracy zdalnej.

Magazyn osobisty na poufne dokumenty

Aby bezpiecznie przechowywać najważniejsze i najbardziej poufne pliki, możesz korzystać z usługi „Magazyn osobisty”. Dokumenty umieszczone w tym archiwum są dodatkowo chronione przez dwuetapową weryfikację i blokowane przed dostaniem się w niepowołane ręce.



Ekspert radzi:

Jak polski sektor MŚP radzi sobie z kwestiami bezpieczeństwa, które zagrożenia są najbardziej niebezpieczne dla małych i średnich firm, które z nich najczęściej dotykają takie firmy. Co robić?

„**Zdaniem eksperta:** Jak polski sektor MŚP radzi sobie z kwestiami bezpieczeństwa, które zagrożenia są najbardziej niebezpieczne dla małych i średnich firm? Jak się przed nimi chronić?

Przedsiębiorcy są coraz bardziej świadomi tych zagrożeń. Utrata środków finansowych, zablokowana strona WWW, wyciek danych klientów to realne konsekwencje cyberataku, dlatego aż **66%** firm jest zainteresowanych zakupem usług zabezpieczających pracowników przed zagrożeniami z internetu, a zaledwie o jeden procent mniej chce zainwestować

w zabezpieczenie firmowych danych. **Taki pakiet usług chroni firmę nie tylko przed cyberatakiem, a również brakiem dostępu do niej wskutek awarii sprzętu czy błędu człowieka.**

Radzę też, by śledzić konto na Twitterze oraz stronę CERT Orange Polska <https://www.cert.orange.pl/mapa>. Na bieżąco publikujemy tam ostrzeżenia o pojawiających się oszustwach i informacje, jak sobie z nimi radzić. **To kolejny sposób na to, by nie paść ofiarą jednego z dwóch milionów cyberataków, jakie mają miejsce dziennie”.**

” **Podstawą ochrony jest wzmożona czujność**



Rafał Wiszniewski

Ekspert ds. cyberbezpieczeństwa

Podsumowanie, czyli **7 zasad** bezpiecznego prowadzenia firmy

- ✓ Bezpieczeństwo firmowych komputerów to nie tylko ochrona przed cyberatakami, lecz również zabezpieczenie przed urazami mechanicznymi, archiwizacja danych i wsparcie IT.
- ✓ Większość uszkodzeń ma miejsce wskutek nieodpowiedniego przenoszenia urządzeń oraz pośpiechu, np. przy wyjmowaniu wtyczki ładowarki czy zamykaniu ekranu.
- ✓ Cyberprzestępcy liczą na Twoją nieuwagę i stosują chwyt socjotechniczne. Nie masz pewności co do autentyczności maila lub SMS-a? Nigdy nie klikaj w link, nie oddzwaniaj i nie przelewaj pieniędzy.
- ✓ Szukasz rozwiązań chroniących zarówno sieć stacjonarną, jak i mobilną? Wybierz CyberTarczę.
- ✓ Zwykle wystarczy 15-minutowa rozmowa ze specjalistą Wsparcia IT, by rozwiązać problem, który laikowi może zająć kilka godzin.
- ✓ Masz wątpliwości, jak przeprowadzić np. aktualizację oprogramowania? Wsparcie IT Ci pomoże, chroniąc przed ryzykiem unieruchomienia komputera.
- ✓ Automatyczne archiwizowanie dokumentów i danych może uchronić Cię przed wieloma problemami. W tym zakresie pomoże Ci Microsoft 365 z usługą OneDrive.

www.orange.pl/poradnik-dla-firm

