Wszystkie firmowe
dane pod kontrolą

orange™

Ochrona danych jest podstawą każdego biznesu, niezależnie od branży i wielkości przedsiębiorstwa.

Na szczęście bezpieczeństwo w firmie można zapewnić bez ponoszenia dużych kosztów związanych z zatrudnieniem specjalisty od cybersecurity.

- Jak chronić firmę przed atakami przestępców?
- W jaki sposób uchronić dane przed konsekwencjami zwykłych błędów pracowników?
- Jakie powinny być najważniejsze zasady bezpieczeństwa w firmie?

Odpowiedzi na te i inne pytania znajdziesz w poniższym e-booku.

1 Dlaczego mała firma powinna mieć wszystkie dane pod kontrolą?

Najsłabszym ogniwem, gdy chodzi o zabezpieczenia w sieci, jest człowiek” – mówi Julien Ducarroz, prezes zarządu Orange Polska, w najnowszym Raporcie CERT Orange Polska za rok 2022. Pracownicy często padają ofiarą cyberprzestępców, którzy podszywając się pod instytucje publiczne i znane przedsiębiorstwa, żerują na ich niewiedzy i nieuwadze.

Wykradzione dane są sprzedawane, mogą posłużyć do szantażu lub wyłudzeń, a także doprowadzić do kradzieży tożsamości czy firmowych pieniędzy.

Utrata danych? Każdemu się może zdarzyć.

Jednak działalność cyberprzestępców to niejedyna przyczyna utraty danych. Często firma traci ważne pliki na skutek ich przypadkowego usunięcia lub zgubienia nośnika danych.

Jak można się dowiedzieć z Global Data Protection Index 2022, **28 proc. przypadków utraty danych ma związek z fizycznym bezpieczeństwem sprzętu, np. jego kradzieżą lub zgubieniem.** Natomiast aż ¼ lub ⅕ danych (w zależności od źródła) ginie na skutek celowego działania pracowników. Zdarza się na przykład, że przed odejściem do konkurencji, pracownik kopiuje bazę danych klientów.

Jak mała firma może utracić dane?

Poznaj najczęstsze przyczyny utraty danych – to pierwszy krok do ich zabezpieczenia.

1. Przypadkowe usunięcie danych.

Może powodować nawet **50%** łącznej utraty danych.

2. Cyberatak na firmę.

Nawet 58% firm odnotowało przynajmniej jeden incydent naruszenia bezpieczeństwa w 2022 roku (dane: Barometr Bezpieczeństwa). – Największy problem – **phishing.**

3. Skopiowanie danych przez osoby nieuprawnione.

Aż 26% przypadków utraty danych ma charakter zamierzonego i celowego postępowania pracowników (dane: Ponemon institute).

4. Awaria lub uszkodzenie sprzętu.

Np. zalanie, upadek, uszkodzenie portów ładowania.

5. Fizyczna kradzież urządzenia.

Średnio co **53 sekundy** kradziony jest laptop (dane: Gartner).

6. Awaria lub niewłaściwie działające oprogramowanie.

50% przypadków przywracania kopii zapasowej kończy się niepowodzeniem.

7. Duże wycieki danych.

W 2022 roku zgłoszono **12,7 tys.** przypadków wycieku danych osobowych (dane: Urząd Ochrony Danych Osobowych).

Danych lepiej nie tracić, ponieważ…

Blokada dostępu do danych lub całkowita ich utrata mogą mieć dla firmy bardzo poważne konsekwencje. Niekiedy przedsiębiorstwo zmuszone jest zawiesić swoją działalność lub nawet ją zakończyć. Do najpoważniejszych konsekwencji należą:

- **Konsekwencje operacyjne.** Czasem utrata jednego pliku paraliżuje funkcjonowanie firmy. Przedsiębiorstwo traci możliwość kontaktu z klientami, prowadzenia rozliczeń, rozwoju produktu lub zmuszone jest wstrzymać produkcję.

- **Konsekwencje rynkowe.** W czasach, gdy obsługa klienta odgrywa kluczową rolę, firma potrzebuje szybkiego i bezpiecznego obiegu informacji dla zachowania konkurencyjności. Przestój w funkcjonowaniu przedsiębiorstwa może też doprowadzić do przejęcia klientów przez konkurencję.

- **Konsekwencje wizerunkowe.** Utrata lub wyciek danych wiąże się również ze stratą zaufania klientów. Szczególnie trudno jest odbudować wizerunek, jeśli działalność firmy wiąże się z usługami medycznymi, finansowymi czy bezpieczeństwem. Co więcej, zaufanie do przedsiębiorstwa tracą nie tylko klienci, ale i sami pracownicy.

- **Konsekwencje finansowo-prawne.** Każda firma, również ta jednoosobowa, w ciągu **72 godzin** ma obowiązek zgłosić wyciek danych osobowych Prezesowi UODO. W przypadku niewielkich uchybień Prezes UODO najczęściej wzywa do poprawy bezpieczeństwa, ale przy powtarzających się lub poważnych wyciekach może on zarządzić karę w wymiarze nawet do **20 mln euro lub do 4 proc. rocznego obrotu z poprzedniego roku.**

Wypowiedź eksperta:

Czy istnieje uniwersalny sposób na zapewnienie firmowym danym ochrony przed różnymi zagrożeniami? Wspólnym mianownikiem dla większości incydentów utraty danych jest brak stosownej wiedzy lub czujności ofiar.

Różnorodne kanały komunikacji mogą ułatwić prowadzenie biznesu, ale tworzą też potencjalne okazje do cyberataku. E-mail, komunikatory, SMS, rozmowa głosowa – tymi drogami wymieniamy dane i każdą z nich może nadejść atak.

Ponadto powinniśmy zdać sobie sprawę, że cyberprzestępcy są niezwykle przebiegli. Wiedzą, z jakimi codziennymi trudnościami borykają się przedsiębiorcy: natłokiem faktur, dużą liczbą wymienianej korespondencji czy wiecznym pośpiechem. I potrafią z każdej z takich sytuacji stworzyć okazję do ataku na nasze dane.

Dlatego, aby zapewnić sobie kontrolę, bezpieczeństwo i ochronę zarówno przed przypadkową utratą danych, jak i cyberatakami, należy zrobić ruch wyprzedzający: **stworzyć zasady, które jasno określą obieg danych w firmie, do firmy i z firmy.**

2 Jednolite zasady bezpieczeństwa – na co zwrócić uwagę?

Choć zdefiniowane w najdrobniejszych szczegółach zasady bezpieczeństwa danych kojarzą się z wielkimi korporacjami o rozbudowanej strukturze IT, warto wdrożyć je także w małej firmie. Każde przedsiębiorstwo powinno posiadać politykę bezpieczeństwa danych, czyli zbiór zasad dotyczących przechowywania, dostępów i obiegu informacji.

Dzięki wdrożeniu polityki bezpieczeństwa danych:

- firma usprawnia swoje funkcjonowanie,
- dostosowuje się do obowiązujących standardów i przepisów prawa,
- znacznie poprawia bezpieczeństwo danych,
- podnosi świadomość i wiedzę pracowników w zakresie cyberbezpieczeństwa.

Zastanówmy się zatem wspólnie, jak powinna wyglądać taka polityka, by z jednej strony była nienadmiernie skomplikowana, a z drugiej – skuteczna.

Podstawowe zasady bezpieczeństwa w małej firmie

Stwórz kompleksowy system ochrony danych na podobieństwo wielkich firm – ale bez wielkich kosztów!

1. Zasada ograniczenia dostępu

- Zastanów się, **kto** faktycznie potrzebuje określonych danych i na tej podstawie przyznawaj dostępy.
- Zminimalizuje to ryzyko przejęcia bądź przypadkowego usunięcia danych.

2. Wykorzystaj pełen potencjał haseł

- Twórz **mocne hasła**, inne dla każdego urządzenia i portalu, z którego korzysta Twoja firma.
- Ustal, **jak często** hasła będą zmieniane, i trzymaj się tego.
- **Żadnych karteczek, zeszytów czy haseł na tablicy** – do przechowywania haseł korzystaj z aplikacji typu menedżer haseł.

4. Kopie zapasowe – element obowiązkowy

- Dane firmowe powinny być **kopiowane regularnie**, jednolitym i wspólnym dla całej infrastruktury w firmie rozwiązaniem.

3. Transport danych? Tylko z zabezpieczeniem

- Dane poufne poza teren firmy, np. na pamięciach USB, mogą być przenoszone tylko odpowiednio zabezpieczone – **hasłem, a najlepiej pełnym szyfrowaniem.**
- Ogranicz transport danych na prywatnych nośnikach.
- Korzystaj z rozwiązań takich jak **VPN**, by zapewnić danym także bezpieczny transport w cyberprzestrzeni.

Podstawowe zasady bezpieczeństwa w małej firmie

Stwórz kompleksowy system ochrony danych na podobieństwo wielkich firm – ale bez wielkich kosztów!

5. Zadbaj o zabezpieczenia przed cyberatakami

- Stosuj oprogramowanie chroniące przed najgroźniejszymi rodzajami cyberataków, przede wszystkim **phishingiem.**
- Na bieżąco aktualizuj swoje zabezpieczenia.

6. Aktualne oprogramowanie to mniej luk bezpieczeństwa

- Wszystkie urządzenia uczestniczące w firmowym obiegu dokumentów powinny mieć **zawsze aktualne oprogramowanie**

7. Edukacja – i to niekoniecznie w postaci drogich szkoleń

- Bądź na bieżąco ze stosowanymi przez cyberprzestępców **metodami.**
- Pomogą Ci w tym takie źródła jak strona CERT Orange Polska i Poradnik dla firm Orange.

3 Wdrażanie zasad bezpieczeństwa jest łatwiejsze z odpowiednimi rozwiązaniami

Edukacja pracowników i spisanie zasad bezpieczeństwa to podstawy prowadzenia bezpiecznego biznesu. Same jednak nie wystarczą. Wiedzy teoretycznej powinny towarzyszyć praktyczne i konkretne działania oraz wdrożenia.

Na szczęście wiele dobrych rozwiązań nie wymaga konieczności całkowitego przeorganizowania działalności. Istnieją usługi i programy, które w profesjonalny sposób pomagają zapewnić bezpieczeństwo w przedsiębiorstwie, a jednocześnie nie wiążą się z dużymi kosztami.

Ochrona przed cyberatakami? Najlepiej kompleksowa

Cyberprzestępcy prześcigają się w wymyślaniu nowych sposobów na phishing – tworzą coraz bardziej profesjonalne strony internetowe, szukają nowych sposobów komunikacji, korzystają z pogłębionych socjotechnik. Wszystko po to, by podszyć się pod wiarygodną osobę, instytucję lub firmę, a następnie wykraść dane lub pieniądze.

Czasem na skutek cyberataku dochodzi także do blokady danych i próby wyłudzenia okupu (ransomware) lub zainfekowania firmowego sprzętu złośliwym oprogramowaniem (malware).

W obronie przed atakami antywirus może okazać się niewystarczający, gdyż nie zawsze chroni on przed atakami socjotechnicznymi. Lepiej sprawdzają się bardziej kompleksowe rozwiązania, jak CyberTarcza od Orange, które blokują większość niebezpiecznych linków i jednocześnie chronią przed kradzieżą wrażliwych danych oraz niechcianymi transakcjami.

Wraz z ewolucją ataków typu phishing, ransomware i malware zmienia się także CyberTarcza – rozwiązania zabezpieczające są nieustannie aktualizowane i wzmacniane.

3-2-1 i… kopia zapasowa gotowa!

Backup danych to rozwiązanie, które okaże się kluczowe w bardzo wielu przypadkach: od awarii sprzętu, przez cyberatak, po nieumyślne usunięcie plików przez pracownika.

Backup powinno się wykonywać według zasady 3-2-1, która mówi: twórz trzy niezależne kopie zapasowe, na co najmniej dwóch różnych rodzajach nośników danych, z których jeden jest przechowywany w innej, niezależnej lokalizacji. Takie niezależne miejsce przechowywania danych zapewniają usługi chmurowe.

Dzięki Backupowi danych od Orange kopie firmowych danych wykonywane są automatycznie i przechowywane w bezpiecznej, polskiej chmurze.

Rozważne przekazywanie danych

Właściciel firmy oraz jej pracownicy powinni zadbać także o bezpieczeństwo swoich prywatnych danych, zwłaszcza numeru PESEL. Podczas wdrażania zasad bezpieczeństwa w firmie warto zwrócić uwagę na takie kwestie jak:

- Komu powierzamy numer PESEL?
- Czy w danej sytuacji jego podanie jest konieczne?
- Czy w skrzynkach e-mailowych i komunikatorach przechowujemy zdjęcia dowodów osobistych lub paszportów?

Kradzież zdjęć to jeden ze sposobów na wykradzenie danych osobowych. Nie należy też ich podawać w sklepach internetowych czy formularzach, których wypełnienie nie jest konieczne.

Warto też regularnie sprawdzać, czy ktoś nie wykorzystuje numeru PESEL np. do wzięcia kredytu na nasze nazwisko. W zachowaniu kontroli nad tym pomoże Ci usługa Zabezpiecz PESEL od Orange.

Szyfrowanie informacji nie jest takie trudne

Szyfrowanie danych polega na ich zakodowaniu, tak by informację odczytać mogła jedynie osoba posiadająca odpowiedni klucz. Dla innych, w tym także hakerów, zaszyfrowany plik będzie miał postać ciągu nic nieznaczących znaków. Szyfrowanie danych osobowych jest zalecaną formą ochrony w rozporządzeniu unijnym RODO. Jednak szyfrować warto nie tylko dane osobowe, ale także inne dane wrażliwe, poufne, takie, które nie powinny dostać się w ręce osób postronnych.

Szyfrowanie jest szczególnie istotne, gdy:

- dane kopiuje się na zewnętrzne nośniki pamięci,
- Ty lub Twoi współpracownicy przemieszczacie się często wraz z firmowymi laptopami.

Choć szyfrowanie danych może się wydawać skomplikowane, dzięki licznym programom wykonuje się je szybko i bezproblemowo. Istnieją programy zapewniające szyfrowanie całych dysków lub pojedynczych plików i folderów.

Wypowiedź eksperta:

Wprowadzenie zasad bezpieczeństwa jest kluczowe, ale jak o nich wszystkich pamiętać?

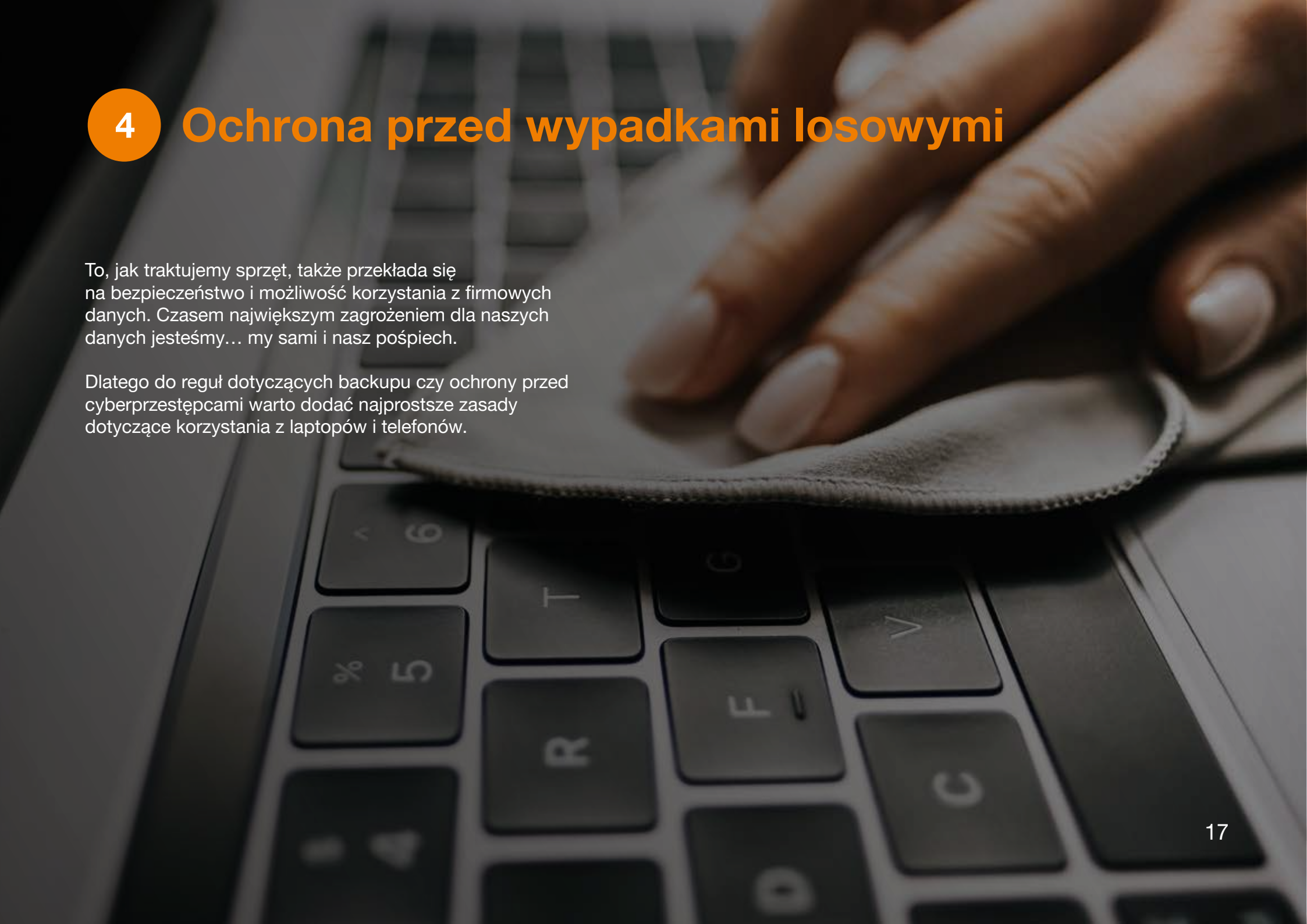
Oczywiście jesteśmy tylko ludźmi i zdarza się nam zapominać o wielu sprawach, szczególnie wśród natłoku faktur, spotkań i służbowych e-maili. Ale i na to są odpowiednie rozwiązania.

To, co stanowi cechę wspólną rozwiązań takich jak **CyberTarcza, Backup danych od Orange** czy **Zabezpiecz PESEL**, to zdjęcie części odpowiedzialności z przedsiębiorcy i umożliwienie mu skupienia się na tym, co najważniejsze w jego działalności.

Dla przykładu: **Backup danych od Orange** pozwala na wykonywanie automatycznych kopii zapasowych wedle ustalonego harmonogramu, dostosowanego do cyklu funkcjonowania firmy. **CyberTarcza** z kolei nie wymaga dokonywania uaktualnień, co jest jej zdecydowaną przewagą nad typowymi antywirusami.

Przy tym są to rozwiązania niedrogie i niewymagające zaawansowanej wiedzy informatycznej do ich obsługi.

4 Ochrona przed wypadkami losowymi

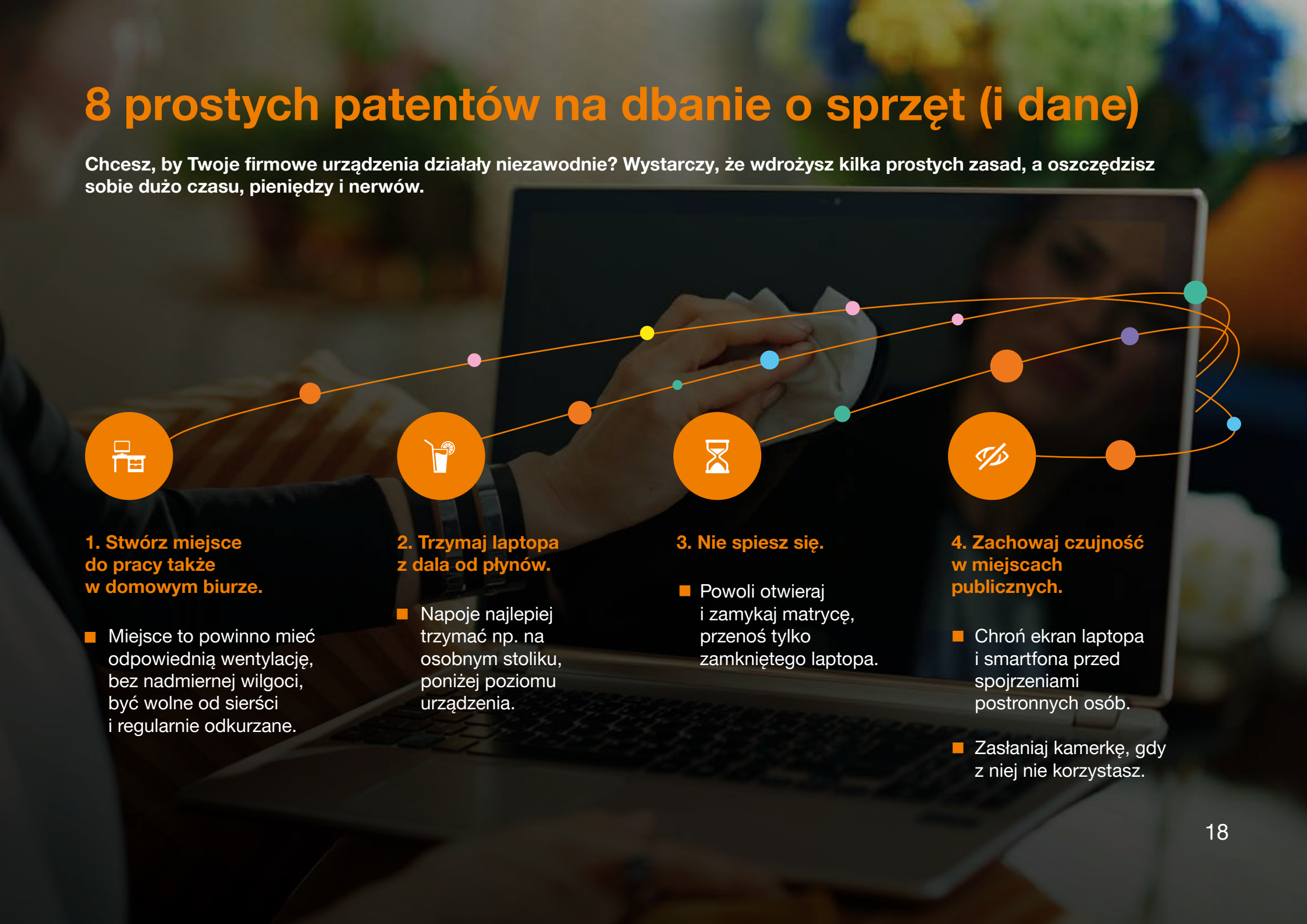


To, jak traktujemy sprzęt, także przekłada się na bezpieczeństwo i możliwość korzystania z firmowych danych. Czasem największym zagrożeniem dla naszych danych jesteśmy… my sami i nasz pośpiech.

Dlatego do reguł dotyczących backupu czy ochrony przed cyberprzestępcami warto dodać najprostsze zasady dotyczące korzystania z laptopów i telefonów.

8 prostych patentów na dbanie o sprzęt (i dane)

Chcesz, by Twoje firmowe urządzenia działały niezawodnie? Wystarczy, że wdrożysz kilka prostych zasad, a oszczędzisz sobie dużo czasu, pieniędzy i nerwów.



1. Stwórz miejsce do pracy także w domowym biurze.

- Miejsce to powinno mieć odpowiednią wentylację, bez nadmiernej wilgoci, być wolne od sierści i regularnie odkurzane.

2. Trzymaj laptopa z dala od płynów.

- Napoje najlepiej trzymać np. na osobnym stoliku, poniżej poziomu urządzenia.

3. Nie spiesz się.

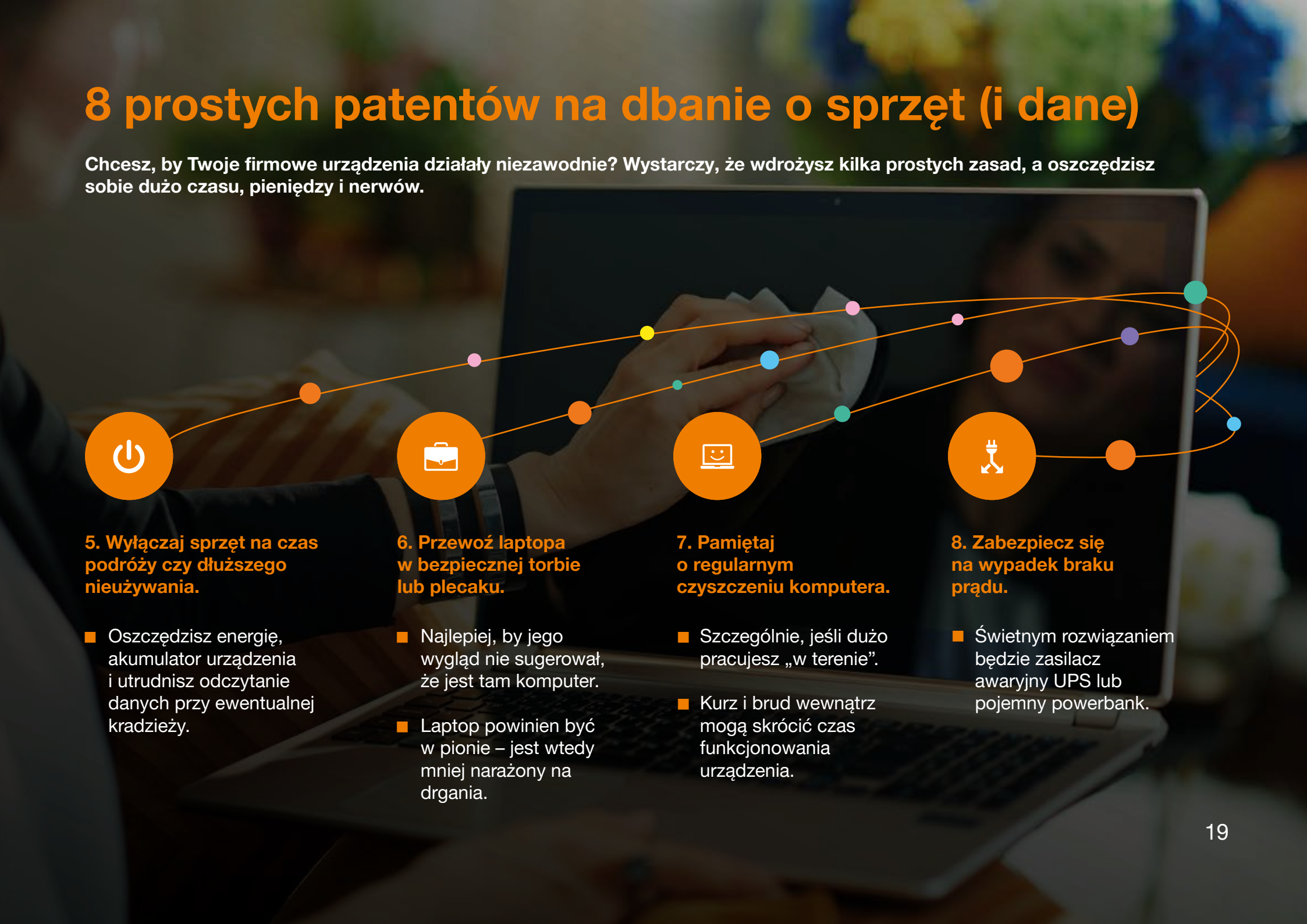
- Powoli otwieraj i zamykaj matrycę, przenoś tylko zamkniętego laptopa.

4. Zachowaj czujność w miejscach publicznych.

- Chroń ekran laptopa i smartfona przed spojrzeniami postronnych osób.
- Zasłaniaj kamerkę, gdy z niej nie korzystasz.

8 prostych patentów na dbanie o sprzęt (i dane)

Chcesz, by Twoje firmowe urządzenia działały niezawodnie? Wystarczy, że wdrożysz kilka prostych zasad, a oszczędzisz sobie dużo czasu, pieniędzy i nerwów.



5. Wyłączaj sprzęt na czas podróży czy dłuższego nieużywania.

- Oszczędzisz energię, akumulator urządzenia i utrudnisz odczytanie danych przy ewentualnej kradzieży.

6. Przewoź laptopa w bezpiecznej torbie lub plecaku.

- Najlepiej, by jego wygląd nie sugerował, że jest tam komputer.
- Laptop powinien być w pionie – jest wtedy mniej narażony na drgania.

7. Pamiętaj o regularnym czyszczeniu komputera.

- Szczególnie, jeśli dużo pracujesz „w terenie”.
- Kurz i brud wewnątrz mogą skrócić czas funkcjonowania urządzenia.

8. Zabezpiecz się na wypadek braku prądu.

- Świetnym rozwiązaniem będzie zasilacz awaryjny UPS lub pojemny powerbank.

A na wszelki wypadek…

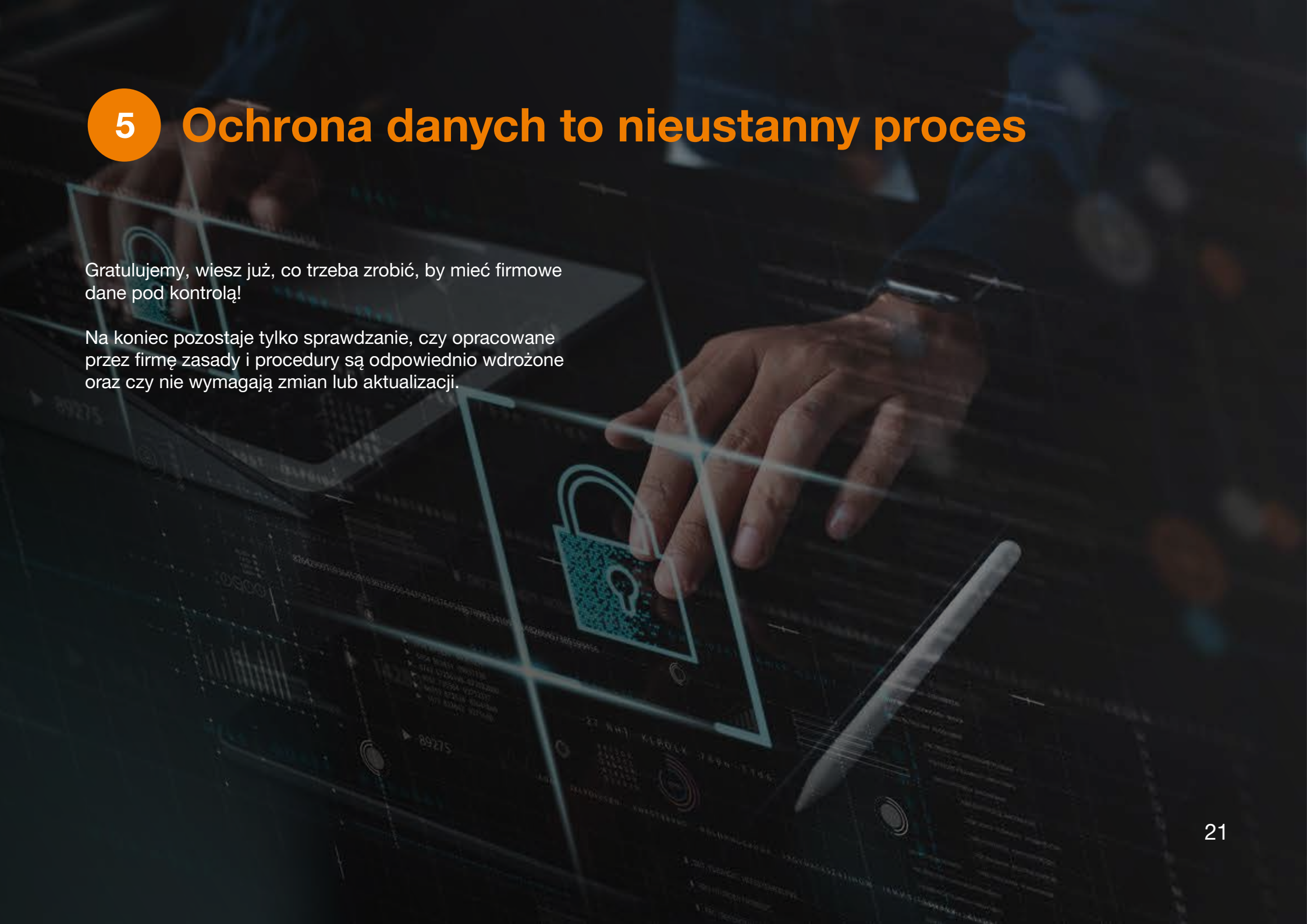
Zasady bezpieczeństwa danych w znaczący sposób ograniczają ryzyko ich utraty, pozwalając spokojnie i bezpiecznie prowadzić biznes. Trudno jednak ustrzec się przed wszystkimi błędami pracowników lub zdarzeniami losowymi.

Dodatkową pomocą „na wszelki wypadek” jest **Wsparcie IT od Orange**. To bardzo pomocna usługa zwłaszcza dla małych i średnich firm, które nie posiadają własnych zespołów IT. Dzięki Wsparciu IT od Orange można uzyskać szybką pomoc zdalną w nagłych wypadkach, a także otrzymać sprzęt zastępczy w awaryjnej sytuacji.

5 Ochrona danych to nieustanny proces

Gratulujemy, wiesz już, co trzeba zrobić, by mieć firmowe dane pod kontrolą!

Na koniec pozostaje tylko sprawdzanie, czy opracowane przez firmę zasady i procedury są odpowiednio wdrożone oraz czy nie wymagają zmian lub aktualizacji.



Do polityki bezpieczeństwa informacji warto wracać i odpowiadać sobie na następujące pytania:

1. Czy wszyscy pracownicy, również nowi, znają zasady bezpieczeństwa obowiązujące w firmie?
2. Czy Ty i Twoi współpracownicy jesteście na bieżąco z technikami wykorzystywanymi przez przestępców?
3. Czy procedury w firmie odpowiadają aktualnym regulacjom, w tym RODO?
4. Czy backup danych odbywa się regularnie, według zasady 3-2-1?
5. Czy programy chroniące firmę przed cyberatakami odpowiadają najnowocześniejszym standardom?
6. Czy przestrzegasz zasady tworzenia haseł i szyfrowania plików?
7. Czy należy uaktualnić zasady dotyczące dostępów?
8. Czy oprogramowanie w firmowym sprzęcie jest aktualne?
9. Czy sprzęt jest regularnie konserwowany i zabezpieczony przed wypadkami?
10. Co wydarzyło się w przypadku cyberataku lub innej sytuacji awaryjnej, czy otrzymałeś odpowiednie wsparcie IT?

Oczywiście trudno zabezpieczyć się przed wszystkim, co może spotkać Twoje firmowe dane. Ale warto pamiętać, że pomoc profesjonalistów połączona z regularnym backupem firmowych informacji sprawia, iż nawet po cyberataku czy awarii sprzętu Twoja firma może praktycznie natychmiast wrócić do gry.

www.orange.pl/poradnik-dla-firm