COMARCH
ERP

Cyberbezpieczeństwo

Wyprzedź hakerów i zadbaj o firmę!

Spis treści

Obraz współczesnych zagrożeń

Podczas gdy firmy przestawiły się na model pracy zdalnej, rynek wysunął na pierwszy plan nowe technologie związane ze współpracą na odległość. Dzięki nim łatwiej zarządzać organizacją, zwiększa się elastyczność i dostępność usług, ale nie wszyscy wykorzystują je w słusznych celach. W dzisiejszych czasach nikt nie jest wystarczająco bezpieczny. Ofiarami ataków cyberprzestępczych padają nawet najwięksi (T-Mobile, Facebook, Marriot – firmy generujące miliardy złotych przychodu, dysponujące ogromnym budżetem na zabezpieczenie sprzętu). Co w takim razie z małymi i średnimi przedsiębiorstwami? One także nie są odporne na cyberataki. Tym bardziej istotne jest, aby zadbać o swoje bezpieczeństwo na wielu płaszczyznach.

Atakujący wykorzystują nowe technologie przede wszystkim w celu pozyskania danych, często także wrażliwych – **danych osobowych, haseł, kluczy, czy numerów telefonów**, aby potem użyć ich przeciwko ich właścicielom: podszywać się pod czyjąś tożsamość, wykraść pieniądze z konta bankowego, czy żądać okupu za ich odzyskanie. Ataki wykorzystujące luki w oprogramowaniu lub sieci mogą spowodować awarię całego systemu, a co za tym idzie, spowodować **paraliż organizacji** i narazić ją nie tylko na wielkie straty finansowe, ale i utratę reputacji. Z raportu Accenture wynika, że 43% ataków wymierzonych jest w **małe i średnie firmy**, z których tylko 14% jest przygotowanych do obrony. Głównie dlatego, że odpowiadają za obrót dużą ilością pieniędzy, a przy tym nie inwestują w cyberbezpieczeństwo swojej firmy.

Konsekwencje mogą być duże także w przypadku naruszenia zasady poufności. Urząd Ochrony Danych Osobowych nałożył na jednego z liderów rynku e-commerce w segmencie dystrybucji elektroniki użytkowej karę w wysokości 2,8 mln zł za to, że dane 2,2 mln klientów sklepu dostały się w niepowołane ręce. Współcześnie do przestępstwa w cyberprzestrzeni dochodzi średnio co 39 sekund.

A jak to wygląda w Polsce?

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku z lipca 2022 roku informuje, że w 2021 roku zarejestrowano **762 185 zgłoszeń** związanych z cyberbezpieczeństwem, a więc ponad trzykrotnie więcej naruszeń niż w roku poprzednim. Fundamentalne aspekty bezpieczeństwa opisuje tzw. triada CIA (z ang. confidentiality, integrity, availability):

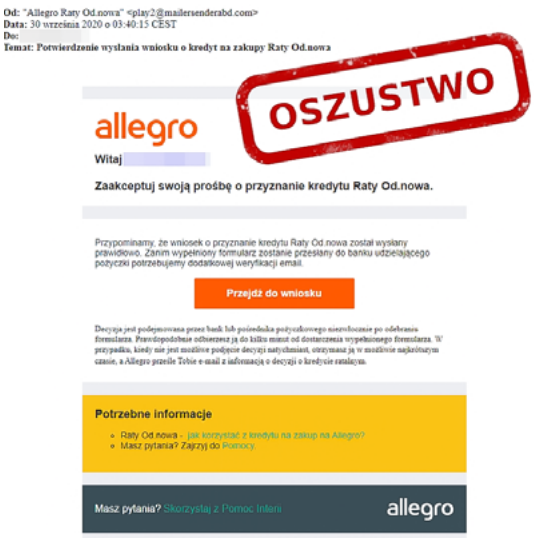
- **poufność** oznacza dostęp do informacji jedynie dla uprawnionych osób,
- **integralność** to ścisłość, wiarygodność oraz zabezpieczenie przed nieuprawnioną modyfikacją,
- **dostępność** oznacza niezawodny dostęp dla uprawnionych osób zawsze, gdy jest potrzebny.

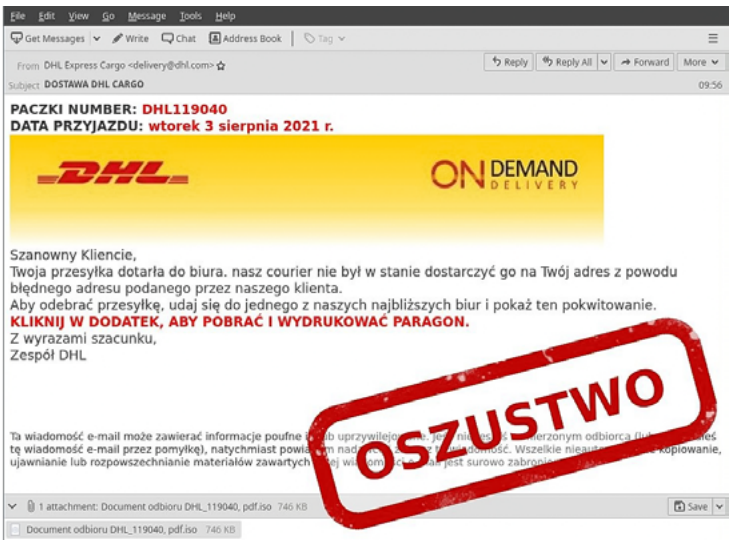
Dużym zagrożeniem dla tych zasad są wszystkie ataki skierowane w kierunku systemów, aplikacji i samych danych. Phishing, ataki typu odmowa usługi, malware, czy ransomware potrafią **sparaliżować pracę organizacji** i narazić ją na duże straty – finansowe i wizerunkowe.

Phishing

Phishing to rodzaj ataku, za pomocą którego haker próbuje wyłudzić od ofiary wrażliwe informacje lub zainfekować komputer użytkownika oprogramowaniem malware.

Najczęstszym rodzajem phishingu jest **phishing e-mail** — haker wysyła wiadomość elektroniczną zawierającą hiperłącze w celu wywołania zaciekawienia lub zaniepokojenia u użytkownika, np. „Paczka oczekuje na dostarczenie, dopłać 2,50 zł, w innym przypadku paczka wróci do nadawcy”. Maile od atakujących są często dopracowane i do złudzenia przypominające te, pochodzące od dobrze nam znanych i zaufanych firm, np.:





Każdego dnia w Internecie wysyłanych jest 3,4 mld maili phishingowych. Google i Threat Analysis Group blokuje każdego dnia około 100 mln takich wiadomości. Cała reszta (w większości) dociera do adresatów.

Wraz ze wzrostem świadomości użytkowników Internetu, wzrasta także kreatywności hakerów. Konsekwentnie tworzone są nowe metody oszustw internetowych, dlatego tak ważne jest, żeby **regularnie aktualizować** swoją wiedzę i być świadomym istniejących zagrożeń.

Phishing również się rozwinął i obecnie mamy kilka jego form:

- **Vishing** — haker dzwoni na telefon domowy, komórkowy lub usługę VoIP i próbuje wciągnąć użytkownika w rozmowę.
- **Smishing** — przestępca wysyła wiadomość tekstową z prośbą o kliknięcie odnośnika lub oddzwonienie do nadawcy.
- **Pharming** — powstał, gdy ludzie nauczyli się rozpoznawać zagrożenie wynikające z klikania odnośników w podejrzanych wiadomościach e-mail. Pharming polega na podsunięciu ofierze adresu URL z nadzieją, że skopiuje go i wklei wprost w pasku adresu przeglądarki, aby wejść na stronę internetową. Spreparowane łącze prowadzi do fałszywej witryny internetowej.
- **Spear phishing** – haker wysyła specjalnie przygotowaną wiadomość e-mail do organizacji lub osoby indywidualnej. Wiadomości typu spear phishing są najczęściej wysyłane do dyrektorów lub pracowników działów finansowych.
- **Whaling** — podobny do spear phishingu, ale jego celem zazwyczaj są osoby z najwyższych stanowisk w firmach.

Statystyki dotyczące **phishingu** opracowane przez Verizon mówią, że 93% udanych cyberataków rozpoczyna się od spear phishingu. Ten typ ataku wymaga od hackera przygotowania, uzyskania informacji o celu ataku. Wyobraźmy sobie sytuację, że do przestrzeni publicznej przedostaje się baza adresów e-mail klientów firmy kurierskiej, wraz z informacją czy klient oczekuje obecnie na dostarczenie przesyłki. Prawdopodobieństwo, że osoba oczekująca na przesyłkę kliknie w link w wiadomości od fałszywej firmy kurierskiej staje się większe.

Warto pamiętać, że pomimo rozwiniętych sposobów ataku, nie jesteśmy tylko biernie patrzącymi ofiarami. Istnieje wiele możliwości, żeby się bronić. Przed kliknięciem w link **należy dokładnie przyjrzeć się** otrzymanej wiadomości e-mail. Najechanie kursorem na źródłowy adres e-mail lub łącze w celu ujawnienia prawdziwych danych, a nie otwieranie linków bez zastanowienia, jest dobrą praktyką. W ten sposób można odkryć

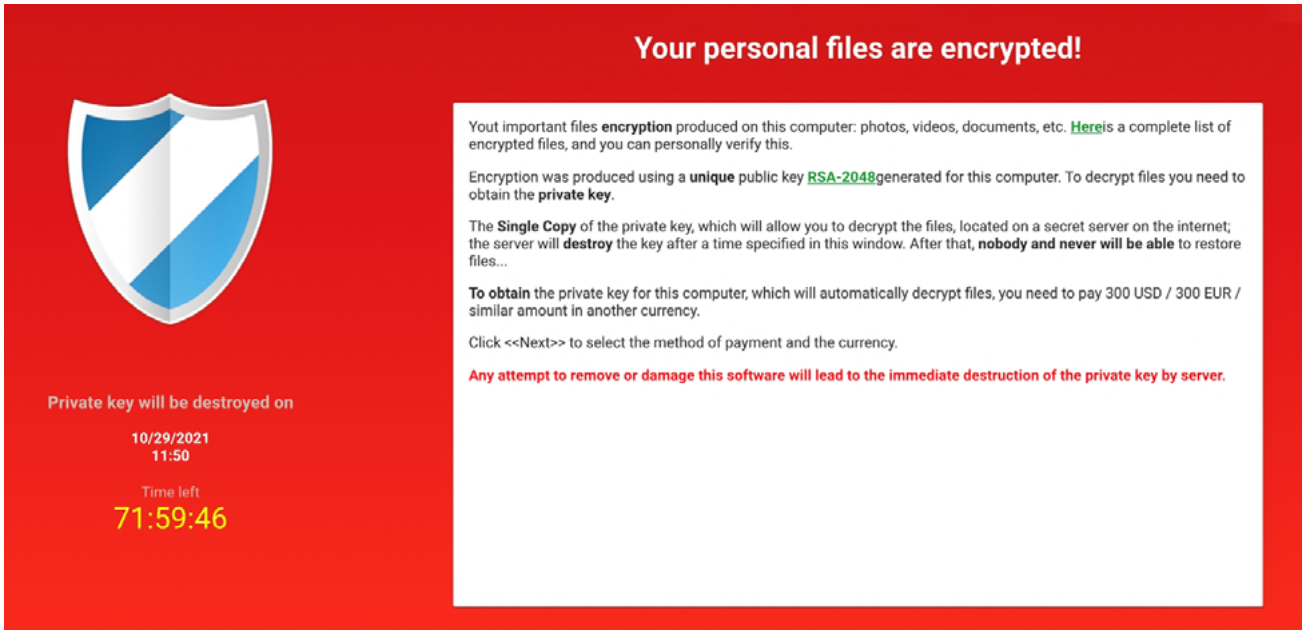
informacje, które pozwolą zorientować się, że to phishing. Przed wpisaniem wrażliwych danych na stronie internetowej, warto dokładnie sprawdzić jej adres URL. **Czy to jest prawdziwa witryna? Czy adres zawiera jakieś dodatkowe litery? Czy niektóre litery zostały zamienione na cyfry, np. O na 0?** Czasami trudno jest je rozróżnić. Przed kliknięciem w link we wpisie opublikowanym przez znajomego należy sprawdzić, czy jest on bezpieczny i zastanowić się, zanim odpowie się na wpis informujący, że znajomy ma kłopoty i potrzebuje pieniędzy. Czy na pewno kontaktowałby się z innymi właśnie w ten sposób? Zagrożenie stanowią także linki w wyskakujących okienkach. Warto pomyśleć, zanim otworzy się załącznik do wiadomości e-mail i zastanowić się przed odpowiedzią na wiadomość SMS. Jest mało prawdopodobne, że operator sieci, bank itp. skontaktują się właśnie w ten sposób.

Ransomware

Większość infekcji złośliwym oprogramowaniem występuje, gdy **nieumyślnie wykonujemy** akcję, która powoduje pobranie złośliwego oprogramowania. Może to być kliknięcie łącza w **wiadomości e-mail** lub odwiedzenie złośliwej witryny internetowej. Jednym z typów złośliwego oprogramowania jest **ransomware**. Zwykle działa on **blokując** lub **odmawiając dostępu do urządzenia i plików**, wymuszając zapłatę okupu hakerowi. Wszelkie osoby lub grupy przechowujące krytyczne informacje na swoich urządzeniach są narażone na zagrożenie ze strony oprogramowania ransomware.

Maksymalizacja zysku z ataku, już nie tylko okup za odszyfrowanie danych, ale też za nieujawnienie informacji o ataku.

Po skutecznym ataku ransomware, po włączeniu komputera jedyne, co jesteśmy w stanie zobaczyć, to ekran informujący o blokadzie oraz informacje o sposobie opłacenia okupu, najczęściej z wykorzystaniem kryptowalut.



Atak polega na wykorzystaniu technik kryptograficznych, więc jeżeli staniemy się jego ofiarą, nasze pliki zostaną zaszyfrowane i niemożliwy będzie ich odczyt bez podania odpowiedniego klucza. I właśnie za podanie tego klucza atakujący **oczekuje opłaty**.

W 2021 roku tylko 4% firm, które zapłaciło okup odzyskało wszystkie dane!

Jakie zatem kroki należy podjąć gdy zostaniemy zainfekowani przez ransomware?

Ważne jest, aby działać szybko. Istnieje kilka kroków, które można podjąć, aby zapewnić możliwie najlepszą szansę zminimalizowania szkód i szybkiego powrotu do normalnego działania.

Oprogramowanie **ransomware**, które atakuje jedno urządzenie, jest umiarkowaną niedogodnością. Oprogramowanie ransomware, które może zainfekować wszystkie urządzenia firmy, to poważny problem. Różnica między nimi często sprowadza się do czasu reakcji. Aby zapewnić bezpieczeństwo sieci, współużytkowania dysków i innych urządzeń, ważne jest, aby **jak najszybciej odłączyć urządzenie**, którego dotyczy problem od **sieci, Internetu i innych urządzeń**. Im szybciej zostanie to zrobione, tym mniej prawdopodobne jest, że inne urządzenia zostaną zainfekowane.

Oprogramowanie ransomware porusza się szybko – szybko dla komputera znaczy coś innego, niż dla człowieka – natychmiastowa izolacja zainfekowanego urządzenia nie gwarantuje, że oprogramowanie ransomware nie istnieje nigdzie indziej w sieci firmy. Aby skutecznie ograniczyć jego zakres, należy **odłączyć od sieci wszystkie urządzenia**, które zachowują się podejrzanie, w tym te działające poza siedzibą firmy – jeśli są podłączone do sieci, stanowią zagrożenie bez względu na to, gdzie się znajdują. Wyłączenie łączności bezprzewodowej (Wi-Fi, Bluetooth itp.) w tym momencie również jest dobrym pomysłem.

Aby określić, które urządzenia zostały zainfekowane sprawdza się ostatnio zaszyfrowane pliki o dziwnych nazwach rozszerzeń plików lub plików, które mają problem z otwieraniem się. Jeśli zostanie znalezione jakiekolwiek urządzenia, które nie zostały całkowicie zaszyfrowane, należy je odizolować i wyłączyć, aby powstrzymać atak i zapobiec dalszym uszkodzeniom i utracie danych. Celem jest stworzenie wyczerpującej listy wszystkich systemów, których dotyczy problem, w tym sieciowych urządzeń pamięci masowej, pamięci

w chmurze, zewnętrznych dysków twardych, laptopów, smartfonów itp. W tym momencie rozsądnie jest zablokować wszystkie akcje, które są wykonywane w systemie. Każda z nich powinna być ograniczona, jeśli to możliwe, a jeśli nie, ograniczona na tyle, ile można. Spowoduje to zatrzymanie wszelkich trwających procesów szyfrowania, a także **zapobiegnie zainfekowaniu** dodatkowych udziałów podczas wykonywania działań naprawczych. Przed tym jednak, należy rzucić okiem na zaszyfrowane pliki. Może to dostarczyć przydatnej informacji: jeśli jedno urządzenie ma znacznie większą liczbę otwartych plików niż zwykle, być może właśnie odnaleziono **Pacjenta Zero**.

Odnalezienie Pacjenta Zero – śledzenie infekcji staje się znacznie łatwiejsze po zidentyfikowaniu źródła. Aby to zrobić, sprawdza się, czy nie ma alertów, które mogły pochodzić z oprogramowania antywirusowego lub dowolnej aktywnej platformy monitorującej. A ponieważ większość oprogramowania ransomware przedostaje się do sieci przez złośliwe łącza i załączniki do wiadomości e-mail, które wymagają działania użytkownika końcowego, przydatne może być również pytanie pracowników o ich działania (takie jak otwieranie podejrzanych wiadomości e-mail) oraz o to, co zauważyli. Wreszcie, spojrzenie na właściwości samych plików może również dostarczyć wskazówki – osoba wymieniona jako właściciel jest prawdopodobnie punktem wejścia.

Identyfikacja oprogramowanie ransomware – ważne jest, aby dowiedzieć się, z jakim wariantem oprogramowania ransomware mamy do czynienia. Jednym ze sposobów jest odwiedzenie **No More Ransom**. Witryna zawiera zestaw narzędzi, które pomogą uwolnić zaszyfrowane dane, w tym narzędzie Crypto Sheriff. Wystarczy przesłać jeden z zaszyfrowanych plików, a zostanie on przeskanowany, aby znaleźć dopasowanie. Po zidentyfikowaniu oprogramowania ransomware i szybkim zbadaniu jego zachowania należy jak najszybciej powiadomić wszystkich niezarażonych pracowników, aby wiedzieli, jak rozpoznać oznaki infekcji.

Ocena kopii zapasowych – teraz nadszedł czas, aby rozpocząć proces reakcji na zagrożenie. Najszybszym i najłatwiejszym sposobem na to jest **przywrócenie systemów z kopii zapasowej**. Idealnie byłoby, gdyby istniała niezainfekowana i kompletna kopia zapasowa utworzona na tyle niedawno, aby była korzystna. Jeśli tak, następnym krokiem jest zastosowanie rozwiązania antywirusowego, aby upewnić się, że wszystkie zainfekowane systemy i urządzenia zostaną wyczyszczone z oprogramowania ransomware – w przeciwnym razie system będzie nadal blokował system i szyfrował pliki, potencjalnie uszkadzając kopię zapasową. Po wyeliminowaniu wszystkich śladów złośliwego oprogramowania będzie można przywrócić systemy z tej **kopii zapasowej** i – po upewnieniu się, że wszystkie dane zostały przywrócone, a wszystkie aplikacje i procesy zostały utworzone i działają normalnie — powrócić do normalnego działania.

Wyciek danych

Celem atakujących coraz częściej są dane – nie tylko te, przetwarzane przez aplikację, ale przede wszystkim **dane wrażliwe – hasła, bazy danych, dane osobowe, czy informacje poufne organizacji**. Często ujawnienie takich informacji kończy się ich **zaszyfrowaniem i żądaniem okupu**.

Jak podaje Business Insider, rekordowa wypłata dokonana przez firmę ubezpieczeniową z tytułu okupu za atak za pomocą oprogramowania blokującego wynosi **40 mln dolarów**. Natomiast w odniesieniu do National Security Institute średnia żądana opłata za okup wzrosła z 500 dolarów w 2018 roku do około 200 000 dolarów. Zapłata okupu nie jest jednak gwarancją odzyskania danych. **80%** ofiar, które zapłaciło przestępcom, wkrótce potem zostało ponownie zaatakowanych, a chociaż 46% z nich uzyskało dostęp do swoich danych, to większość była uszkodzona.

Przykładów wśród nas jest wiele. W styczniu 2020 roku na skutek błędnej konfiguracji serwera atak spowodował wyciek danych ponad **250 mln rekordów** z bazy danych **Microsoft** z danymi klientów firmy z okresu **14 lat** jej działalności. Wyciek ujawnił adresy e-mail, adresy IP i inne dane dotyczące klientów.

Kiedy globalna pandemia zbierała coraz większe żniwo, wszyscy przestawili się na zdalne formy komunikacji, pracy i nauki. Wtedy w **dark webie** [1] pojawiła się oferta sprzedaży danych **500 mln loginów i haseł użytkowników** aplikacji Zoom. Ze względu na niski stopień zabezpieczeń w szybkim tempie rozpowszechniło się zjawisko włamań i zakłóceń przebiegu (teoretycznie) prywatnych konferencji. Po tym zdarzeniu reputacja Zoomu ucierpiała mocno, a niektóre organizacje zakazały używania tej aplikacji jako formy służbowej komunikacji.

W tym samym roku wyciekły dane klientów linii lotniczej EasyJet. Firma stanęła w obliczu zbiorowego pozwu założonego przez klientów dotkniętych naruszeniem danych. Jego wartość oszacowano na **18 mld funtów**. W marcu 2021 roku hackerzy wykorzystali podatności w konfiguracji Microsoft Exchange, które rzutowały na systemy pocztowe i kalendarzowe. W ten sposób napastnicy uzyskali dostęp do wiadomości e-mail oraz haseł użytkowników, uprawnień administratora na zaatakowanym serwerze oraz dostęp do podłączonych urządzeń w tej samej sieci. Microsoft szybko wydał łatkę bezpieczeństwa, jednak szkód nie udało się usunąć. Wkrótce potem ofiarami włamania zostały parlament Norwegii oraz firma Acer, od której zażądano okupu w wysokości 50 mln dolarów.

Jeden z największych ataków typu **data leak** to rok 2021 i firma **Facebook**. W sieci znalazły się dane ponad **533 mln** użytkowników portalu Facebook ze 106 krajów, w tym także Polski. Mimo upływu czasu nadal można je znaleźć i pobrać z GitHuba lub grup w serwisie Telegram. Nietypowy okup, bo w formie usunięcia wprowadzonej funkcji uniemożliwiającej wydobywanie kryptowalut (Lite Hash Rate) ze swoich nowych kart graficznych, a także udostępnienie kodu źródłowego sterowników na licencji open source, zażądali atakujący od firmy NVIDIA. Atak ransomware w lutym 2022 roku został dokonany przez grupę Lapsus$, która potwierdziła, że uzyskała dostęp do 1 TB danych. Sprawcy ataku poinformowali, że wykradli ponad **70 000 adresów e-mail** pracowników i haseł, a także informacje o jeszcze nieogłoszonych procesorach, SDK i kodzie źródłowym GPU.

---

[1] Dark Web – termin określający najciemniejszą stronę Internetu, do której zwykły użytkownik nie może się dostać z poziomu tradycyjnej przeglądarki internetowej. Z Dark weba korzystają przestępcy tacy jak handlarze narkotyków, broni, terroryści oraz każdy, kto czepie korzyści z faktu bycia anonimowym.

Jak się przed tym chronić?

Na **bezpieczeństwo powinno się zwracać uwagę** na każdym etapie produkcji – poprawnie skonfigurowane systemy operacyjne, zasada minimalnych uprawnień, okresowy przegląd infrastruktury, korzystanie z aktualnego oprogramowania zabezpieczającego. Warto ćwiczyć świadome i bezpieczne surfowanie po sieci i zwracać uwagę, gdzie się klika, a także nie odpowiadać na e-maile i SMS-y od nieznanych osób i pobierać aplikacje tylko z zaufanych źródeł. Jest to ważne, ponieważ autorzy złośliwego oprogramowania często **używają socjotechniki**, aby skłonić ofiarę do zainstalowania niebezpiecznych plików.

Dobrą praktyką jest wdrożenie programu uświadamiającego bezpieczeństwo oraz zapewnienie **regularnych szkoleń** dotyczących świadomości bezpieczeństwa wszystkim członkom organizacji, aby mogli uniknąć phishingu i innych ataków socjotechnicznych. Warto przeprowadzać regularne ćwiczenia i testy, aby mieć pewność, że wytyczne ze szkolenia są przestrzegane.

Kopie zapasowe

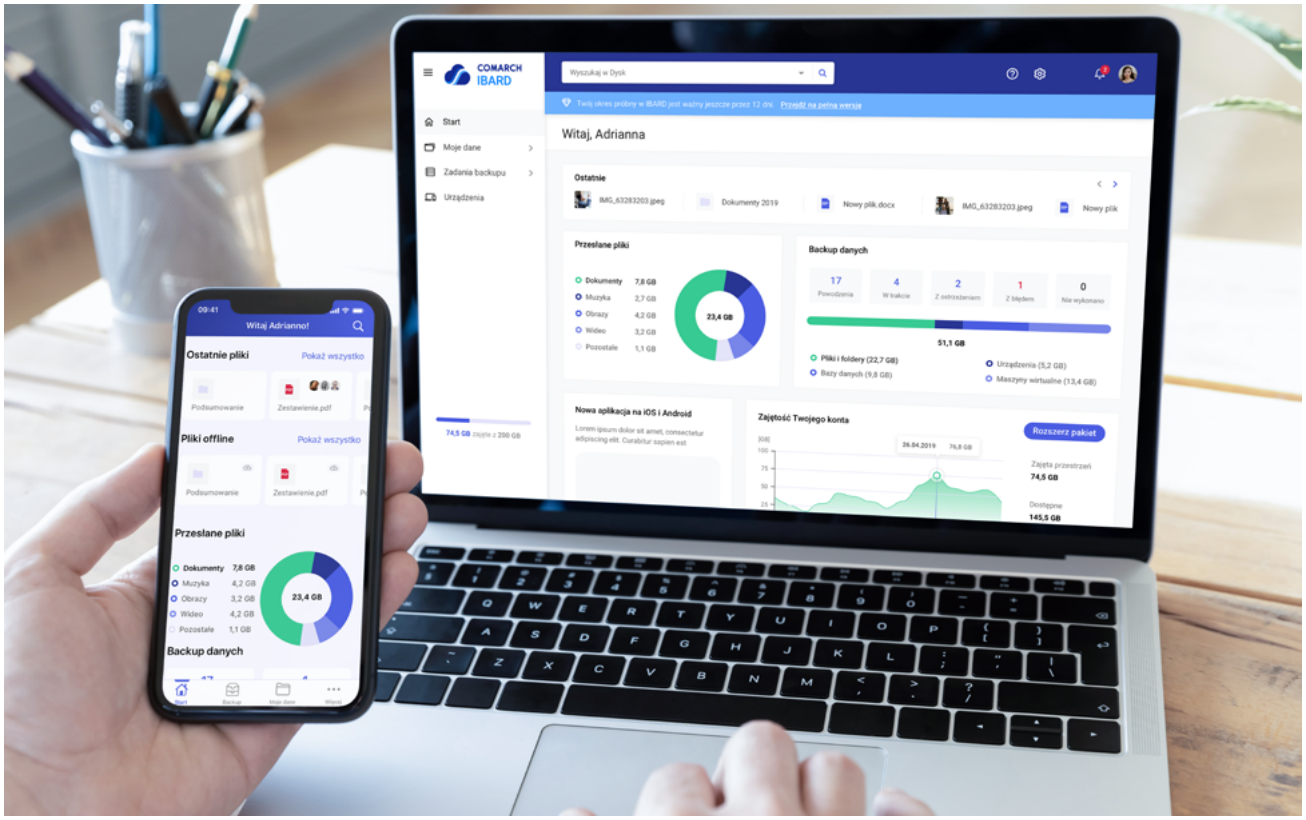
Backupy, czyli kopie bezpieczeństwa, zapewnią nas, że nie utracimy dostępu do danych, kiedy zostaną one naruszone. Kopiować można zarówno bazy danych, jak i fizyczne serwery. Dobrze działający **backup** uchroni nas przed zatrzymaniem cyklu produkcyjnego, paraliżem organizacji, czy nawet nieumyślnym usunięciem ważnych danych. Choć nie uchroni bezpośrednio przed wyciekiem informacji jako skutku ataku, przygotowanego w precyzyjny sposób przez hackera, tak jednak **zmniejszy straty i skutki** takiego działania. Kopie zapasowe nie zapobiegną oprogramowaniu ransomware, ale mogą zmniejszyć ryzyko.

Znanym powiedzeniem w świecie cyberbezpieczeństwa jest hasło: „kopia zapasowa jest na tyle bezpieczna, na ile da się z niej odtworzyć dane”. Wynika z niego, iż bez okresowych testów dostępności zapisanych danych nie

możemy być pewni, iż po incydencie będziemy w stanie je odtworzyć. Warto pamiętać, że same **kopie zapasowe** także mogą stać się obiektem ataku – szczególnie, jeśli nie są w żaden sposób odseparowane od środowiska, które może paść celem ataku ransomware. **Kopie zapasowe** mogą mieć różną postać: od dysków systemowych i wymiennych dysków twardych, po urządzenia taśmowe offline i **kopie zapasowe w chmurze**. Wszystkie z nich powinny być należycie chronione i zabezpieczone. Warto upewnić się, że dane kopii zapasowej nie są dostępne do modyfikacji lub usunięcia z systemów, w których znajdują się dane. Ransomware może wyszukać niezabezpieczone kopie zapasowe danych i zaszyfruje je lub usunie, aby nie można ich było odzyskać. Dobrą praktyką jest wykorzystywanie formy backupu, która nie pozwala na bezpośredni dostęp do plików kopii zapasowych.

Standardem w dziedzinie backupów jest **zasada 3-2-1**, a więc minimum **trzy kopie** na **dwóch urządzeniach** oraz **co najmniej jedna** kopia przechowywana w innej lokalizacji niż dane oryginalne podlegające zabezpieczeniu. Dostosowanie się w praktyce do zasady 3-2-1 zapewnia usługa **Comarch IBARD**, która w bardzo prosty sposób umożliwia skonfigurowanie zadania backupu oraz harmonogramu jego wykonywania. **Comarch IBARD** działa w tle i wykonuje automatycznie backupy według ustalonych reguł.

Zasada 3-2-1



Comarch IBARD

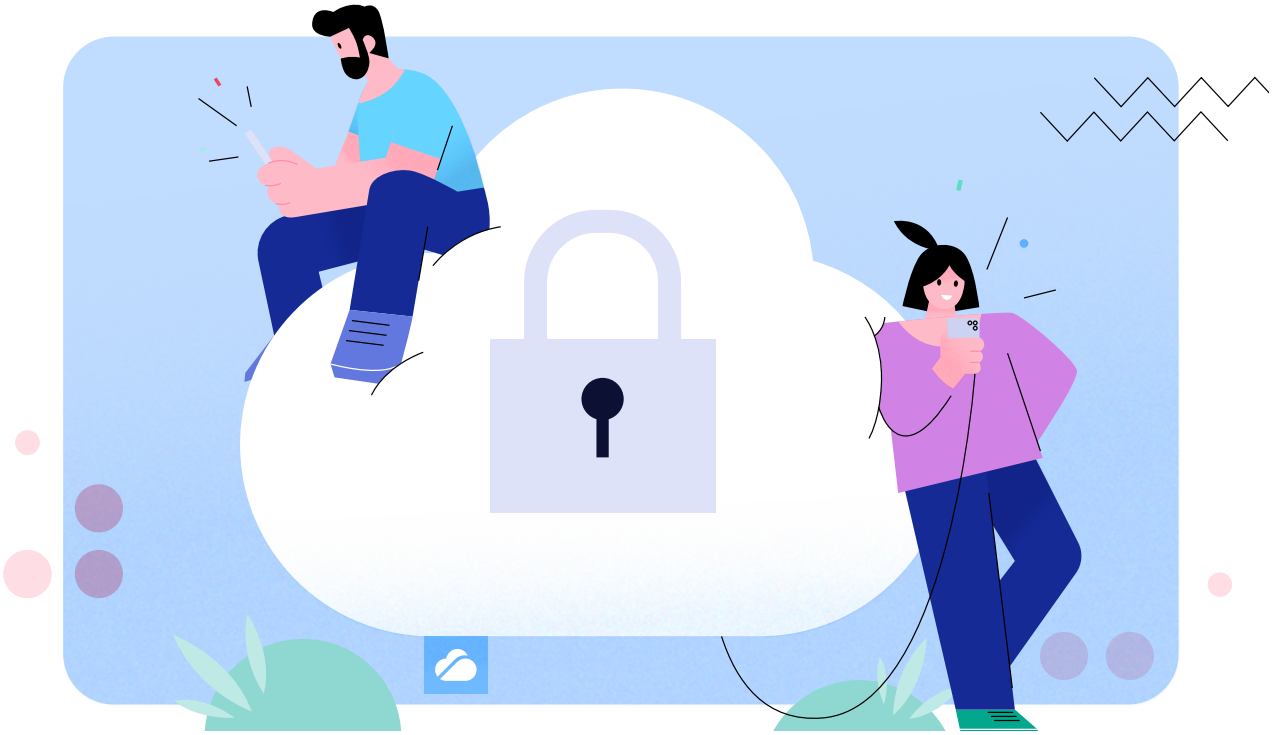
Comarch codziennie przetwarza terabajty danych, stanowiących tajemnicę handlową działalności biznesowej swoich klientów. Mając na uwadze ich **zaufanie**, na pierwszym miejscu stawia **bezpieczeństwo i ochronę** ich przed nieuprawnionym dostępem z zewnątrz.

Comarch IBARD to w stu procentach **polska chmura** dla firm - aplikacja umożliwiająca bezpieczny i intuicyjny **backup danych**, zarówno z komputerów jak i urządzeń mobilnych. Pozwala na przechowywanie danych w chmurze, ich synchronizację, wersjonowanie i pracę nad dokumentami w czasie rzeczywistym na dowolnym urządzeniu.

Szyfrowanie za pomocą **protokołu SSL** zapewnia bezpieczeństwo transmisji przesyłania danych do **Comarch IBARD**. Dzięki niemu masz pewność, że w czasie połączenia twój transfer jest szyfrowany i nikt niepowołany nie będzie miał dostępu do twoich danych. Nawet jeśli hakerom uda się zainfekować dane i będą żądali okupu, to dzięki rozwiązaniu od **Comarch** informacje są bezpieczne i w każdej chwili mogą zostać przywrócone. Ponad to **Comarch IBARD** umożliwia szyfrowanie danych za pomocą klucza prywatnego u samego użytkownika (Comarch IBARD używa klucza AES-256). Dzięki temu nie ma możliwości, że dane zostaną odczytane przez dostawcę usług.

Comarch IBARD umożliwia także trzymanie kopii w innej lokalizacji niż nasza baza danych (w chmurze), tak więc w przypadku ataku na bazę – **kopia będzie bezpieczna** – choćby dlatego, że jest mało prawdopodobne, żeby zarówno baza i kopia były zaatakowane jednocześnie.

W celu skutecznego zabezpieczenia się przed ransomware potrzebne jest tworzenie regularnych kopii zapasowych. Intuicyjny i elastyczny kreator harmonogramu zadań backupu w **Comarch IBARD** pozwala na nieograniczoną ilość konfiguracji zadań backupu. Rozwiązanie jest tak proste, że nie wymaga pomocy działu IT i pozwala pracownikom na indywidualne ustawienie zadań.



Nie ma skuteczniejszego środka na ochronę przed skutkami ransomware niż **kopie zapasowe**. Średni koszt okupu w 2021 roku to równowartość 1-1,5 BTC, czyli na chwilę obecną 240-360 tys. zł. **Comarch IBARD dla klientów ERP kosztuje 240 zł/rocznie.** Wybierz mądrze.

COMARCH

KONTAKT

Odwiedź www.comarch.com, żeby uzyskać więcej informacji o naszych biurach w wybranych krajach:

Albania
Austria
Belgia
Brazylia
Kanada
Chile
Chiny
Finlandia
Francja
Niemcy
Włochy
Luksemburg
Malezja
Panama
Polska
Rosja
Hiszpania
Szwajcaria
Turcja
UAE
Wielka Brytania
Ukraina
USA

Comarch Spółka Akcyjna z siedzibą w Krakowie, Aleja Jana Pawła 39 a, zarejestrowana w Krajowym Rejestrze Sądowym prowadzonym przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000057567.

Wysokość kapitału zakładowego Spółki wynosi 8.133.349,00 zł. Kapitał zakładowy wpłacony w całości.

info.erp@comarch.com **www.comarch.pl/erp**