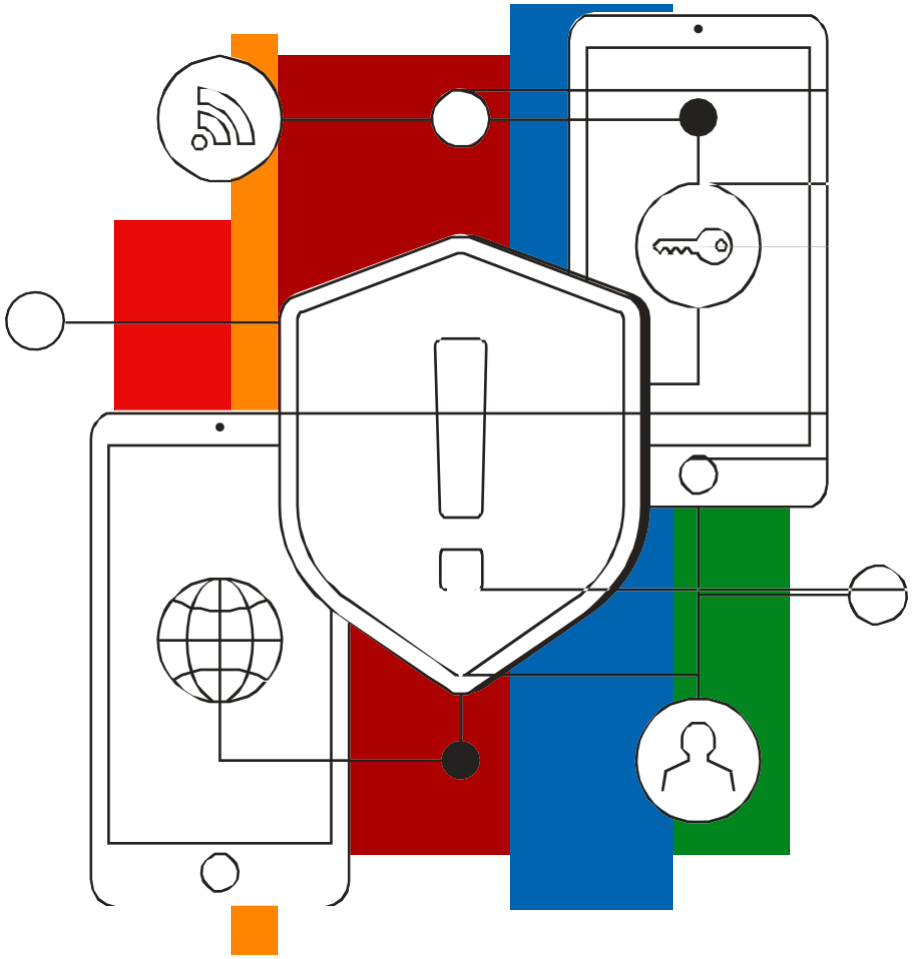

Dobre praktyki bezpieczeństwa

dla przedsiębiorców
opracowane przez mBank S.A.

Wstęp

Ataki cyberprzestępców są dużym wyzwaniem dla bezpieczeństwa informatycznego firm. Mogą prowadzić do wycieku danych, naruszać bezpieczeństwo poufnych informacji oraz powodować, że systemy informatyczne przestaną działać.

Odpowiednie zabezpieczenia i higiena bezpieczeństwa są niezbędne, by uchronić się przed tego typu incydentami. Pomagają one uniknąć poważnych konsekwencji prawnych i finansowych, strat wizerunkowych oraz utraty zaufania klientów i partnerów biznesowych.

Stosuj zasady bezpieczeństwa!

najczęstsze przyczyny cyberataków

phishing

Phishing polega na tym, że oszuści rozsyłają wiadomości (np. e-maile, SMS-y) z linkami do fałszywych stron lub z niebezpiecznymi załącznikami. W ten sposób podstępem wyłudzają poufne dane, np. login i hasło do konta w banku czy dane osobowe.

O czym należy pamiętać:

- zawsze sprawdzaj adresy e-mail nadawców, np. czy nie ma w nich literówek
- jeśli masz wątpliwości, czy wiadomość jest wiarygodna, skontaktuj się z nadawcą w inny sposób (np. telefonicznie)
- zwróć uwagę na format załączników z wiadomości – szczególnie uważaj na pliki, które mają w nazwie kilka rozszerzeń (np. faktura_10.pdf.exe, przelew.pdf.zip, wyplata.jar.doc), takie pliki mogą zainfekować Twoje urządzenie złośliwym oprogramowaniem
- zanim klikniesz w link w e-mailu, najedź na niego myszką, aby zobaczyć, dokąd kieruje i upewnij się, że adres URL jest prawidłowy

złośliwe oprogramowanie

Aby zmniejszyć ryzyko infekcji złośliwym oprogramowaniem:

- korzystaj tylko z zaufanych źródeł – nie pobieraj oprogramowania i aplikacji z podejrzanych stron internetowych i zawsze sprawdzaj reputację źródła
- przed instalacją nowego oprogramowania, przeskanuj je za pomocą aktualnego programu antywirusowego
- regularnie skanuj urządzenie programem antywirusowym, aby wykryć i usunąć potencjalne zagrożenia, regularnie przeprowadzaj też pełne skanowanie systemu urządzenia oraz ustaw harmonogram skanowań
- stosuj zaawansowane rozwiązania do ochrony stacji roboczych – oprócz programów antywirusowych rozważ stosowanie również oprogramowania typu Endpoint Protection, które pozwala wykryć bardziej zaawansowanych metod infekcji twoich komputerów

niezabezpieczone usługi sieciowe

Zabezpieczaj usługi sieciowe:

- sprawdź, czy Twoje urządzenia nie udostępniają niepotrzebnych usług sieciowych do internetu takich jak np. pulpit zdalny – jeśli nie jest to absolutnie konieczne, ogranicz taki dostęp
- upewnij się, że sieć Wi-Fi, z której korzystasz jest zabezpieczona silnym algorytmem szyfrowania oraz silnym hasłem, nie udostępniaj osobom trzecim sieci wykorzystywanej do pracy
- upewnij się, że wszystkie połączenia z kluczowymi aplikacjami odbywają się za pomocą bezpiecznych protokołów, takich jak np. HTTPS – zapewniają one szyfrowanie transmisji danych, co chroni je przed podsłuchiwaniem i modyfikacją

wykorzystywanie luk w oprogramowaniu

- aplikacje i programy pobieraj tylko z oficjalnych sklepów, nie pobieraj ich z niezaufanych źródeł
- zadbaj o aktualizacje systemu operacyjnego swojego urządzenia, żeby mieć zawsze najnowszą wersję – to pozwoli wyeliminować luki bezpieczeństwa
- śledź informacje o nowych podatnościach i zagrożeniach publikowane przez producentów oprogramowania oraz zaufane źródła branżowe, to pozwoli Ci szybko reagować na potencjalne zagrożenia
- sprawdzaj bezpieczeństwo oprogramowania, które dostarczają Ci firmy zewnętrzne – luki bezpieczeństwa w takim oprogramowaniu mogą spowodować zainfekowanie ransomewere Twojej sieci.

urządzenia USB

Korzystaj jedynie z urządzeń z zaufanych źródeł:

- podłączaj do komputera/laptopa tylko te urządzenia USB, które pochodzą z zaufanych źródeł
- przeskanuj urządzenie USB zanim otworzysz jakikolwiek zapisany na nim plik – użyj programu antywirusowego lub oprogramowania typu Endpoint Protection
- wyłącz funkcję autoodtwarzania plików na komputerze – złośliwe oprogramowanie nie uruchomi się automatycznie
- nie zostawiaj urządzenia bez opieki, szczególnie w miejscach publicznych lub tam, gdzie inne osoby mogą mieć do niego dostęp
- ogranicz użycie pendrive'ów i przenośnych dysków, rozważ, czy wszyscy pracownicy firmy potrzebują używać tego typu urządzeń

współdzielenie komputera

Współdzielenie komputera może zwiększyć ryzyko. Aby temu zapobiec:

- nie udostępniaj urządzeń używanych do pracy swoim dzieciom lub innym członkom rodziny
- do prywatnych celów używaj innego urządzenia

korzystaj z bezpiecznych urządzeń

Zadbaj o bezpieczeństwo urządzeń (np. laptopów, telefonów), na których Ty i Twoi pracownicy lub współpracownicy przetwarzają informacje poufne.

Korzystaj z urządzeń sieciowych z uruchomionym systemem firewall.	Firewall skonfiguruj tak, by ograniczyć ruch sieciowy do niezbędnego minimum, co zmniejszy ryzyko nieautoryzowanego dostępu.
Regularnie instaluj poprawki bezpieczeństwa.	Upewnij się, że regularnie aktualizujesz system operacyjny urządzeń oraz oprogramowanie, aby zabezpieczyć się przed najnowszymi zagrożeniami. To samo dotyczy sieciowych urządzeń brzegowych, takich jak firewalle, routery i koncentratory VPN.
Ogranicz uprawnienia użytkowników.	Zablokuj użytkownikom urządzeń uprawnienia tak, by nie mogli zmieniać konfiguracji, instalować, deinstalować i uruchamiać nieautoryzowanego oprogramowania. Nie zezwalaj także na nieautoryzowaną wymianę danych z innymi urządzeniami, jeśli zadania pracownika tego nie wymagają.
Automatycznie blokuj urządzenia.	Ustaw automatyczne blokowanie dostępu do systemu operacyjnego po maksymalnie 15 minutach bez aktywności użytkownika. To pomoże zapobiec nieautoryzowanemu dostępowi.
Zabezpiecz zdalny dostęp do sieci wewnętrznej za pomocą szyfrowanego połączenia VPN.	Zapewnia ono dodatkową warstwę bezpieczeństwa – ukrywa ruch sieciowy i utrudnia dostęp do sieci osobom niepowołanym. Pamiętaj, że VPN to jedna z wielu warstw ochrony, choć zwiększa prywatność, nie chroni przed wszystkimi zagrożeniami.

Zabezpiecz urządzenia przed kradzieżą i nieuprawnioną ingerencją.

Włącz audyt zdarzeń	Pozwoli to jednoznacznie zidentyfikować użytkownika, który wprowadził zmiany w systemie informatycznym.
Ustal indywidualne hasła dostępu.	Zapewnij, by każdy użytkownik urządzenia miał swoje indywidualne hasło dostępu. Ogranicz dostęp do systemów i danych do minimum niezbędnego, by wykonywać pracę.
Stosuj polityki silnych haseł.	Zadbaj o to, by hasła zabezpieczacie urządzenia tworzyć zgodnie z najlepszymi praktykami rynkowymi. Używaj długich (co najmniej 12 znaków), losowych haseł, które są trudne do odgadnięcia.

Zadbaj o bezpieczeństwo urządzeń (np. laptopów, telefonów), na których Ty i Twoi pracownicy lub współpracownicy przetwarzają informacje poufne.

Nie zezwalaj na współdzielenie kont.	Wprowadź zakaz współdzielenia kont przez współpracowników. Dzięki temu zapobiegniesz nieautoryzowanemu dostępowi i braku rozliczalności z działań danego użytkownika.
Ogranicz dostęp do zasobów sieciowych.	Ogranicz dostęp do zasobów sieciowych tylko do określonych urządzeń lub użytkowników. Zminimalizujesz w ten sposób ryzyko nieautoryzowanego dostępu.
Ogranicz dostęp do konta administratora.	Konta administratora (również na stacji roboczej) nie wykorzystuj do codziennej pracy. Upewnij się, że Twoi pracownicy korzystają z konta administratora tylko wtedy, gdy potrzebują go, by wykonać zadanie.
Wyłącz wbudowane i nieużywane konta.	Zadbaj o to, by wyłączyć konta, których nie wykorzystujecie do pracy (np. konto gościa).
Dwuskładnikowe uwierzytelnianie (2FA)	Włącz dwuskładnikowe uwierzytelnianie na kontach i usługach, tam gdzie tylko jest to możliwe. 2FA wymaga dodatkowego potwierdzenia tożsamości, co znacząco utrudnia przejęcie kont przez nieuprawnione osoby. Korzystaj z rozwiązań dostarczanych przez renomowanych dostawców, dzięki czemu zmniejszysz ryzyko nieuprawnionego dostępu do przetwarzanych informacji.
Korzystaj z menedżerów haseł.	Pomagają one generować, przechowywać i stosować silne hasła. Pamiętaj jednak, żeby odpowiednio zabezpieczyć także dostęp do menedżera.

twórz bezpieczne kopie zapasowe

Kopie zapasowe pozwalają na szybkie przywrócenie danych, jeśli złośliwe oprogramowanie zaszyfruje Twoje urządzenia.

Zdecyduj, co chcesz zabezpieczyć.	Kopia zapasowa powinna uwzględniać najważniejsze dane lub cały obraz systemu, by w razie potrzeby można było szybko przywrócić pełną funkcjonalność.
Twórz kopie zapasowe regularnie.	Dzięki temu zmniejszysz ryzyko utraty danych. Zastanów się, jak długo Twoja firma może działać bez najnowszych danych. Czy poradzisz sobie, gdy stracisz dane z kilku ostatnich dni? Na tej podstawie ustal, jak często potrzebujesz tworzyć kopie zapasowe.
Przechowuj kopie zapasowe na zewnętrznych nośnikach, odłączonych od sieci, zasilania i głównego systemu.	Dzięki temu zminimalizujesz ryzyko zainfekowania kopii przez złośliwe oprogramowanie, które może się rozprzestrzenić na wszystkie dostępne dyski i zasoby sieciowe. Odizolowanie kopii zapasowych zapewni Ci dostęp do czystej, nieuszkodzonej wersji danych.
Zapewnij bezpieczny dostęp do kopii zapasowych.	Upewnij się, że dostęp do kopii zapasowych mają tylko uprawnieni użytkownicy.
Regularnie testuj odtwarzanie z kopii zapasowych.	Regularnie sprawdzaj, czy kopie zapasowe są kompletne i czy można je bezproblemowo przywrócić. Dzięki temu będziesz mieć pewność, że kopie są użyteczne w sytuacjach kryzysowych.
Szyfruj kopie zapasowe.	W ten sposób zabezpieczysz dane na wypadek kradzieży urządzenia lub nośnika, na którym jest kopia. Przechowuj klucz odzyskiwania w bezpiecznym miejscu, niezależnym od szyfrowanego urządzenia i zewnętrznych zasobów z kopiami zapasowymi.

chroń informacje poufne

Bezpieczeństwo informacji poufnych Twojej firmy w dużej mierze zależy od osób, które w niej pracują. Zadbaj o to, by Twoi pracownicy i współpracownicy wiedzieli, jak chronić takie informacje.

Zapewnij formalną ochronę informacji poufnych.

Wprowadź regulację wewnętrzną, w której określisz najważniejsze zasady, na jakich bezpiecznie przetwarzacie informacje poufne.

Podaj w niej:

- które informacje są poufne, jak z nimi postępować i jak je zabezpieczać,
- gdzie wyrzucać dokumenty papierowe, komu można je przekazywać, jak z nimi postępować podczas pracy zdalnej czy w podróży.

Wprowadź pisemne zobowiązanie do zachowania poufności.

Zadbaj o poufność Twoich informacji przetwarzanych przez pracowników i współpracowników. Wprowadź obowiązek składania przez nich oświadczenia o zachowaniu poufności. Może to być oddzielne oświadczenie lub zapis w umowie zawieranej z pracownikiem lub współpracownikiem. Dzięki temu upewnisz się, że każdy kto przetwarza informacje poufne, wie o tym.

Buduj świadomość pracowników i współpracowników.

Zadbaj, aby osoby przetwarzające informacje poufne w Twojej organizacji, wiedziały, jak to robić. Cyklicznie organizuj szkolenia, w których wskażesz najważniejsze zasady, np. jak. postępować z takimi informacjami, komu mogą je przekazywać, jak je zabezpieczać, jeśli mają być przekazane poza Twoją firmę, na co uważać (np. linki i załączniki w wiadomościach e-mail, instalacja oprogramowania z nieznanego źródła). Rozważ zakończenie szkolenia krótkim testem.

Wprowadź procedurę obsługi incydentów.

Wprowadź regulację wewnętrzną, w której określisz, w jaki sposób obsługiwać incydenty bezpieczeństwa.

Podaj w niej:

- co w Twojej organizacji jest incydentem,
- gdzie i w jaki sposób zgłosić incydent,
- kto powinien się zająć incydentem i jakie działania wykonać,
- do kogo w firmie cyklicznie zgłaszać informację o incydentach.

Wprowadź procedurę obsługi podatności.

Wprowadź regulację wewnętrzną, w której określisz, w jaki sposób obsługiwać podatności w Twoim środowisku teleinformatycznym.

Podaj w niej:

- jak klasyfikować podatności,
- w jakich terminach usuwać podatności,
- gdzie i w jaki sposób zgłaszać podatności,
- kto powinien koordynować usuwanie podatności,
- do kogo w firmie cyklicznie zgłaszać informację o nieusuniętych podatnościach.

korzystaj z bezpiecznego oprogramowania

Kieruj się najlepszymi, aktualnymi praktykami bezpiecznego wytwarzania oprogramowania. Stosuj zasady bezpieczeństwa bez względu na to, czy wytwarzasz oprogramowanie samodzielnie, czy zamawiasz je od zewnętrznego dostawcy.

Zadbaj o bezpieczeństwo architektury. Korzystaj z oprogramowania tworzonego zgodnie z koncepcjami ochrony poufnych informacji:	▪ **secure by design** – projektowanie systemu tak, by już w fazie projektu uwzględniać wymogi bezpieczeństwa adresujące ryzyka jakie system mógłby bez nich stwarzać dla przetwarzanych w nim informacji, ▪ **defence in depth** – projektowanie wielowarstwowej ochrony systemu dla bezpieczeństwa przetwarzanych w nim informacji, ▪ **secure by default** – wbudowanie właściwej ochrony informacji poufnych w strukturę projektowanego systemu tak, by system ją wymuszał – domyślnie obowiązuje ona bez dodatkowych czynności, ▪ **default deny** – domyślna odmowa dostępu – dostęp musi być udzielony świadomie, jawnie i być rozliczany, ▪ **fail secure** – projektowanie systemu tak, by po jego uszkodzeniu lub błędzie samoczynnie przechodził w stan, który zapobiega utracie jego bezpieczeństwa (np. uniemożliwia dostęp do informacji), ▪ **zero trust** – podejście, które zakłada, że nie można ufać żadnemu komponentowi, urządzeniu ani sieci, niezależnie od tego, czy znajdują się wewnątrz, czy poza organizacją.
Stosuj najlepsze praktyki bezpiecznego kodowania	(np. obejmujące wytyczne „OWASP TOP 10 Proactive Controls”).
Zadbaj o ochronę danych osobowych. Wdrażaj rozwiązania oparte o koncepcje:	▪ **privacy by design** – projektowanie systemu tak, by już w fazie projektu uwzględniać ochronę prywatności danych osobowych, ▪ **privacy by default** – wbudowanie właściwej ochrony prywatności w strukturę projektowanego systemu tak, by system ją wymuszał – domyślnie obowiązuje ona bez dodatkowych czynności,

Unikaj wykorzystywania niedojrzałych lub wygasłych/nierozwijanych technologii.

Testuj oprogramowanie przed jego wdrożeniem na środowisku produkcyjnym oraz gdy wprowadzasz w nim istotne zmiany.	Sprawdzaj je nie tylko pod kątem funkcjonalności i wydajności, ale przede wszystkim bezpieczeństwa (tzw. pentesty).

dbaj o bezpieczeństwo fizyczne

Zadbaj o to, aby niepowołane osoby nie dostały się do Twojego biura i nie spowodowały szkód (np. nie wyniosły poufnych dokumentów).

Wprowadź kontrolę dostępu.	Wprowadź np. elektroniczne wejściówki do pomieszczeń, w których Twoja firma przetwarza informacje poufne lub o dużym znaczeniu biznesowym. Kontroluj dostęp także do pomieszczeń, w których jest sprzęt informatyczny (np. laptopy, drukarki, serwery). Dzięki temu będziesz wiedzieć, kto i kiedy przebywa w poszczególnych pomieszczeniach.
Monitoruj wizyty gości.	Zadbaj o to, by rejestrować wizyty osób spoza Twojej firmy. Przede wszystkim dotyczy to gości, którzy będą w pomieszczeniach, w których jest sprzęt biurowy lub dokumenty z poufnymi informacjami. Takie osoby powinny poruszać się po firmie w towarzystwie pracownika Twojej firmy.
Rozważ monitoring wizyjny.	Rozważ wdrożenie systemu monitoringu wizyjnego pomieszczeń, w których Twoja firma przetwarza informacje poufne lub o dużym znaczeniu biznesowym. Weź pod uwagę także pomieszczenia, w których jest sprzęt informatyczny (np. laptopy, drukarki, serwery).
Zabezpiecz dokumenty.	Jeśli pracownicy i współpracownicy w Twojej firmie posługują się papierową dokumentacją, zadbaj o to, aby odpowiednio ją zabezpieczali po zakończonej pracy (np. zabierali je z drukarek i biurek oraz odkładali do zamykanej na klucz szafy lub sejfu). Dzięki temu osoby nieuprawnione (np. osoby sprzątające pomieszczenia) nie będą miały wglądu w te dokumenty.