Poradnik dla małych i średnich przedsiębiorstw

Opracowali:

Robert Siudak – Instytut Kościuszki
Artur Marek Maciąg – Inicjatywa Kultury Bezpieczeństwa
Janusz Żmudziński – Polskie Towarzystwo Informatyczne
Michał Rosiak – Orange Polska

Materiał został opracowany przez Zespół ds. małych i średnich przedsiębiorstw w ramach pracy Grupy roboczej ds. Cyberbezpieczeństwa działającej przy Ministerstwie Cyfryzacji

Spis treści

I. Wstęp

Nie warto demonizować cyberzagrożeń. Bezpieczeństwo w sieci to nic trudnego. Wystarczy niewiele, by w znaczący sposób ograniczyć ryzyko utraty wrażliwych danych Twoich, czy Twojej firmy. Zwróć uwagę, że bezpieczeństwo cyfrowe to wyzwanie dla trzech podstawowych sfer:

1. **Twoich procesów biznesowych** –uwzględniaj zagrożenia związane z bezpieczeństwem IT w trakcie planowania swojej codziennej działalności;
2. **Ciebie i Twoich współpracowników** – klucz do tego tkwi przede wszystkim w Twojej głowie i w Twoich emocjach;
3. **Technologii jakie stosujesz** – pamiętaj, że są one tylko narzędziami, używaj ich z głową a w razie potrzeby znajdź specjalistę, który pomoże Ci nad nimi zapanować;

Poniżej znajdziesz szereg porad dotyczących tego jak wzmocnić swoje bezpieczeństwo cyfrowe w tych trzech wymiarach.

II. Cyberbezpieczeństwo to wyzwanie dla twoich procesów biznesowych

Chroń cenne zasoby firmy, czyli informacje.

Każda firma posiada zdigitalizowane informacje, które może traktować jak swoje srebra rodowe. Mogą to być np. informacje finansowe, dane klientów, informacje techniczne, wyniki badań naukowych. Utrata tych informacji może być katastrofalna dla firmy. Każde przedsiębiorstwo powinno w pierwszej kolejności przeprowadzić inwentaryzację informacji, aby wiedzieć z jakimi danymi mamy do czynienia. Krytyczne dane powinny być szczególnie chronione.

Zarządzaj bezpieczeństwem i ryzykiem.

Każdy pracownik w przedsiębiorstwie może stać się przypadkowym współsprawcą ataku na system informatyczny firmy. Może doprowadzić do zainfekowania go złośliwym oprogramowaniem, klikając spreparowane linki zwarte w poczcie elektronicznej lub uruchamiając załączniki przygotowane przez cyberprzestępców. Stworzenie bezpiecznego przedsiębiorstwa wymaga zaangażowania wszystkich pracowników. Wskazane jest budowanie kultury świadomego ryzyka związanego z określeniem ryzyka i celów, a następnie rozpowszechnianie informacji dot. cyberbezpieczeństwa w całej firmie. Zalecane jest przeprowadzanie cyklicznych ćwiczeń dla wszystkich pracowników mających dostęp do systemu informatycznego firmy.

Zarządzanie zdarzeniami i reagowanie na incydenty związane z bezpieczeństwem to zadanie dla wszystkich, nie tylko działu IT.

Zdarzenia mające wpływ na stan cyberbezpieczeństwa w firmie mogą mieć miejsce w różnych obszarach przedsiębiorstwa i różnych miejscach jego systemów informatycznych. Co więcej mogą być ze sobą powiązane. Niezbędny jest wysiłek całej firmy aby monitorować takie zdarzenia, np. korzystając z zautomatyzowanych systemów, i szybko reagować na wykryte incydenty bezpieczeństwa.

Pamiętaj o bezpieczeństwie już na etapie projektowania lub zakupu systemu IT.

Jedna z największych słabości systemów informatycznych - i w konsekwencji strat finansowych – związana jest z pomijaniem kwestii bezpieczeństwa na etapie projektowania tych systemów. Niestety wciąż częste są sytuacje, że najpierw wdraża się usługi a dopiero później dodaje się rozwiązania bezpieczeństwa. Bardzo wskazanym rozwiązaniem jest budowanie bezpieczeństwa od początku projektu. Takie podejście nie tylko zwiększa poziom bezpieczeństwa, ale również oszczędza pieniądze.

Zarządzaj tożsamością użytkowników i dostępem do informacji.

Ważnym elementem zapewnienia cyberbezpieczeństwa w przedsiębiorstwie jest zarządzanie cyklem życia tożsamości. Obejmuje ono wszelkie działania związane z:

- rozpoczęciem cyklu (utworzenie kont, wprowadzenie danych),
- zarządzaniem zmianami (zmiany danych, zmiany uprawnień),
- zakończeniem życia tożsamości w organizacji (zablokowanie, usunięcie kont, odebranie dostępu, ujednolicenie informacji o zakończeniu życia tożsamości we wszystkich systemach).

Firmy, które źle zarządzają tożsamościami, mogą być narażone na włamania. Zagrożeniu temu można zaradzić poprzez wdrożenie rzetelnych systemów identyfikacji osób, które pozwalają na zarządzanie uprawnieniami dostępu do informacji i anulowania ich gdy pracownicy odchodzą z firmy.

Korzystaj z bezpiecznych kanałów komunikacji.

Firmy nieustannie komunikują się z kontrahentami, klientami lub wymieniają informacje pomiędzy swoimi biurami. Bezpieczeństwo komunikacji powinno być integralnym elementem systemu teleinformatycznego. Może być zrealizowane z wykorzystaniem łatwych w użyciu mechanizmów kryptograficznych, np. szyfrowania poczty elektronicznej, szyfrowanego kanału komunikacji (SSL), w szczególności jeżeli mamy do czynienia z informacjami istotnymi biznesowo.

Ograniczaj słabe punkty.

Cyberprzestępcy stale poszukują słabych punktów, które mogą być przydatne do ataku na system informatyczny. Słabe punkty (podatności) są częstą przypadłością systemów informatycznych współczesnych przedsiębiorstw. Dlatego niezwykle ważne jest aktualizowanie oprogramowania. Przestarzałe oprogramowanie, zwłaszcza w złożonych systemach ułatwia życie cyberprzestępcom. Co gorsza, twórcy oprogramowania czasami przestają tworzyć poprawki do starszych wersji programów. Cyberprzestępcy dobrze o tym wiedzą. W bezpiecznym systemie administratorzy powinni na bieżąco aktualizować wykorzystywane oprogramowanie, zwłaszcza instalować dostępne poprawki bezpieczeństwa.

Oceniaj i testuj bezpieczeństwo swojej firmy.

Kultura bezpieczeństwa przedsiębiorstwa powinna uwzględniać cykliczną ocenę i testy bezpieczeństwa wykorzystywanych systemów informatycznych. Jest to proces analogiczny do kontroli jakości.

III. Cyberbezpieczeństwo to wyzwanie dla Ciebie i Twoich współpracowników

Nie traktuj dbałości o bezpieczeństwo jako dodatkowego obowiązku w pracy.
Świadomość zagrożeń w sieci przede wszystkim pomoże na co dzień Tobie i Twoim najbliższym. Unikniesz maili phishingowych, nauczysz dzieci odpowiedzialnego korzystania z mediów społecznościowych, a seniorów przeszkolisz w aspekcie tego, na co powinni uważać w internecie. To, czego się nauczysz i wprowadzisz w życie, przyda Ci się na wielu płaszczyznach. Praca to tylko jedna z potencjalnych korzyści.

Używaj menedżera haseł.
Tego typu oprogramowanie pozwala Ci tworzyć bardzo długie, losowe hasła do serwisów internetowych. Pamięta je i wpisuje za Ciebie, gdy należy się zalogować. Ty musisz zapamiętać tylko jedno – wtedy bezdyskusyjnie bardzo mocne – hasło do menedżera oraz kilka haseł do kluczowych serwisów jak e-mail, bank, czy serwisy społecznościowe. Przykłady rozwiązań tego typu: Lastpass, KeePass, 1Password.

Tam, gdzie możesz, włącz uwierzytelnianie dwuskładnikowe.
Jeśli serwis, z którego korzystasz, pozwala na to, uruchom uwierzytelnianie dwuskładnikowe (2 Factor Authentication, 2FA). Polega ono na wprowadzeniu dodatkowego składnika uwierzytelniania, poza podstawowym hasłem. Możliwości 2FA to: hasło SMS, hasło w mailu, zmieniane co 60 sekund hasło w dodatkowej aplikacji (np. Google Authenticator), bądź

akceptacja logowania na komputerze przy użyciu urządzenia mobilnego. Listę serwisów wspierających 2FA znajdziesz na https://twofactorauth.org/.

Dokładnie przyglądaj się wiadomościom z „grup ryzyka".
Dokładnie czytaj każdą wiadomość (e-mail/SMS), która ma związek z kontami w serwisach internetowych, czy płatnościami, zawiera linki i/lub załączniki. Przyjrzyj się adresowi nadawcy, jakości treści, najedź (bez klikania!) na łącza w e-mailu i sprawdź, czy ukryte pod nimi linki prowadzą do odpowiedniej domeny. Sprawdzaj tzw. tiny url, czyli skrócone adresy stron internetowych na dedykowanych do tego celu portalach. Nie wpisuj swoich danych wrażliwych na stronach, których nie znasz. Nie klikaj w załączniki w mailach, o ile nie masz absolutnej pewności co do źródła ich pochodzenia.

Spiesz się powoli.
Przestępcy są coraz lepszymi socjotechnikami, wiedząc, że odniosą sukces dopiero wtedy, gdy przekonają Cię do instalacji złośliwego programu. Dlatego grają na naszych emocjach, sugerując m.in. konieczność opłacenia przesyłki, zapłaty zaległej faktury, bądź drobnej zaległości finansowej, nierzadko szantażując potencjalną ofiarę odebraniem dostępu do usługi, czy wręcz karą pieniężną, czy przekazaniem informacji organom ścigania. Uspokojenie emocji ułatwi nam wyłapanie psychologicznych sztuczek.

Wprowadź w firmie procedurę postępowania z mailami z „grup ryzyka".
Określ zamkniętą grupę tego typu informacji (dostawca usług telefonicznych/internetu, dostawcy mediów, kontrahenci biznesowi). Przekaż pracownikom wzory otrzymywanych od nich maili listę adresów nadawców oraz – w przypadku korespondencji cyklicznej – ramowe terminy otrzymywania maili. Zobowiąż pracowników do zgłaszania jakichkolwiek odstępstw od procedury przed podjęciem wobec nich jakiejkolwiek aktywności.

Staraj się unikać łączenia życia zawodowego z prywatnym w sieciach społecznościowych.
Poznanie ofiary to pierwszy krok do udanego phishingu. Wiedza o tym, gdzie pracujesz i/lub czym się interesujesz, z kim przyjaźnisz – to wszystko może znacznie ułatwić spreparowanie maila, na którego niemal na pewno zareagujesz, czy to kliknięciem w link, czy otwarciem załącznika. Pamiętaj o odpowiednich ustawieniach prywatności – we wszystkich sieciach społecznościowych możesz zawczasu zdecydować, kto będzie mógł widzieć Twoje posty.

Bądź odpowiedzialny w internecie.
Pamiętaj, że w sieci anonimowość nie istnieje, a treści które się tam raz pojawią raz, zostają na zawsze. Prędzej, czy później, nasze nieodpowiedzialne zachowania mogą zostać wyciągnięte na jaw. Pół biedy jeśli popsują opinię wyłącznie nam – gorzej, jeśli wpłyną na postrzeganie naszego pracodawcy lub zainteresują organy ścigania.

IV. Cyberbezpieczeństwo to wyzwanie dla technologii których używasz

1. Taktyka i praktyka stosowania technologii

Poznaj technologię - zbuduj bazę używanych technologii i zasobów, ustal standard konfiguracji
Technologia używana w firmie może stanowić jej atut oraz być jej słabą stroną. To jaka będzie w Twoim wypadku zależy od tego na ile dobrze ją znasz i kontrolujesz. W tym celu upewnij się, że posiadasz listę wszystkich technologii używanych do wspierania ludzi i procesów, zarówno w Twoim biurze jak i poprzez zewnętrzne firmy. Możesz zacząć od prostej listy zawierającej np. nazwę technologii wraz z wersją, jej dostawcę, wymogi licencyjne, opiekuna w Twojej firmie (lub kogoś kto podejmuje decyzje z nią związane i ma kontakt z jej dostawcą), administratora, ogólnie jej użytkowników.

Kolejnym krokiem jest ustalenie i utrzymywanie typowej dla Ciebie konfiguracji (np. stacji roboczej pracowników) dla danej technologii. W ten sposób uprościsz jej zarządzanie i skrócisz czas potrzebny do odzyskania ciągłości działania w przypadku pomyłki, jak również dasz sobie szansę na wykrycie nieautoryzowanych zmian - jednej z oznak ataku na Twój biznes.

Chroń dane - monitoruj podatności technologiczne, poznaj ograniczenia i problemy, ustal kontrole
Technologia podlega ciągłym zmianom i musisz być przygotowany (-a) na koszt operacyjny związany z jej utrzymaniem. Posiadając informacje o stosowanych technologiach możesz ustalić które jej elementy będą samoczynnie się aktualizować, a które wymagają ustalenia procesu zarządzania zmianą. Stwórz listę używanego oprogramowania i urządzeń sieciowych. Upewnij się, które z nich automatycznie pobierają z sieci uaktualnienia, dla pozostałych ustal harmonogram regularnego sprawdzania stron producentów pod kątem łat bezpieczeństwa.

Poznaj swoje słabe strony - twoja technologia ma też ograniczenia.
Każda technologia posiada pewne ograniczenia, które mogą zagrozić stabilności lub bezpieczeństwu Twoich usług. Do takich ograniczeń między innymi należą: podatności protokołów komunikacyjnych wymagających dodatkowych zabezpieczeń (http->https), szkolenia pracowników w zakresie użytkowania interfejsu technologii (np. detekcja phishingu przez pracowników), podatności samych systemów operacyjnych na złośliwe oprogramowanie i nieautoryzowane zmiany czy dostęp (oprogramowanie ochronne dla sieci, serwerów i końcówek użytkownika, jak: systemy detekcji i prewencji IPS/IDS, systemy anty-malware - AV, systemy ochrony przed wyciekiem danych - DLP). Pamiętaj, że mobilność Twoich pracowników, czy zdalne przetwarzanie danych oznacza konieczność

ochrony danych przed kradzieżą, wymagające np. stosowania szyfrowania całości nośników i higieny stosowanych nośników wymiennych.

Zrozum działanie swoich systemów - ustal zakres monitoringu usług cyfrowych w twojej firmie, zdefiniuj co jest normą, monitoruj aktywność użytkowników.
Kluczem bezpiecznego stosowania technologii do wspierania biznesu jest ciągły monitoring ich funkcjonowania. To zadanie można realizować samodzielnie, można też zlecić zewnętrznej organizacji, czy odpowiednio zaprojektowanej technologii (np. usługom chmurowym). W celu ochrony Twojego biznesu, bardzo ważne jest monitorowanie aktywności użytkowników, zarówno Twoich pracowników jak i aktywności wszelkiego rodzaju partnerów. Warto w tym celu ustanowić jakie zdarzenia w obrębie stosowanych technologii oznaczają stan normalny, a które z nich wymagają uwagi jako potencjalny incydent bezpieczeństwa danych w Twojej firmie. Do skutecznej realizacji tego zadania potrzebujesz informacji o stanie technologii, np. poprzez zbieranie istotnych dla Twoich celów logów. Przydatną może również okazać się technologia (lub usługa) analizy logów i zautomatyzowanego raportowania o anomaliach (tzw. SIEM i podobne).

Reaguj na incydenty - stwórz plan reakcji na incydenty i przetestuj go.
Szybka reakcja na incydent, najczęściej stanowi o tym, czy Twój biznes będzie nadal się rozwijał czy też pogrążą go skargi, kary i odszkodowania. Najważniejszym etapem reakcji na incydent z użyciem technologii jest przygotowanie do niego. Posiadanie samego planu również nie wystarcza, plan należy testować, tak aby osoby i technologie w nim kluczowe były sprawdzone, sprawne i dostępne gdy zdarzy się incydent. Zanim wejdziesz w interesy z innym usługodawcą, sprawdź jak pomoże Ci w przypadku incydentu (oraz jakich i ile doświadczył incydentów po swojej stronie).

Skuteczny plan oprzeć można na 6 podstawowych fazach: identyfikacji, oceny, ograniczenia wpływu, eliminacji zagrożenia, przywrócenia usług do stanu normalnego oraz analizy przyczyn i wyciągnięcia wniosków. Powinien on zostać również uzupełniony o dane dotyczące technologii i kanałów komunikacyjnych niezbędnych w czasie incydentu, zaangażowania osób technicznych wraz z instrukcjami postępowania, skonfigurowania technologii przed, a nie w trakcie incydentu, w tym ustalenia procedur wymiany informacji pomiędzy Tobą a stroną trzecią (np. gwarancję informacji o incydencie u usługodawcy zewnętrznego, gdy incydent dotyczy danych Twojego biznesu przez nich przetwarzanych).

W razie incydentu odzyskaj zdolność do działania – rób kopie zapasowe, nie używaj urządzeń mobilnych do składowania danych.
Incydenty i błędy są konsekwencją użytkowania technologii i należy uwzględnić je w swoim modelu biznesowym. Ludzie dzielą się na tych, którzy robią backupy i tych, którzy będą je robić. Bądź mądry przed szkodą, twórz regularnie kopie zapasowe, w przypadku danych kluczowych – na urządzeniach nie podłączonych na stałe do sieci. Dzięki temu

w przypadku, gdy nie uda się uniknąć np. zaszyfrowania danych przez ransomware, możliwe będzie ich szybkie i bezbolesne odtworzenie. Pamiętaj, że kopia zapasowa danych musi być składowana w innym miejscu czy urządzeniu w którym zazwyczaj dane te są przetwarzane.

Zapewnij, że kluczowe media i zasoby dostarczone są z „zapasem" niezbędnym do utrzymania zdolności do dostarczenia usług, w przypadku awarii standardowych zasobów czy ataku odmowy usługi. Pomocne mogą być odpowiednie usługi firm zewnętrznych, w tym umowy o gotowości. Pamiętaj również, że urządzenia mobilne (smartfony, tablety itp.) to urządzenia do tymczasowego przetwarzania a nie składowania danych, oraz częściej ulegają zniszczeniu czy zagubieniu niż atakowi.

2. Strategia i zarządzanie technologiami

Nie ufaj – kontroluj dostęp, ustaw bezpieczne hasło, stosuj zapory sieciowe
Bez względu na to jaką technologię używasz, daje ona dostęp do danych od których zależy Twój biznes. Upewnij się, że technologia ogranicza dostęp do danych i funkcji jedynie osobom które tego potrzebują do pracy. Tworzenie furtek "na wszelki wypadek" czy nie zamykanie dostępu po gościach to wymarzone okazje dla przestępców. Pamiętaj aby zarządzać użytkownikami i ich uprawnieniami, najlepiej centralnie, z użyciem np. technologii Active Directory czy Menadżera Tożsamości, dla łatwiejszych przeglądów. Upewnij się, że każde uprzywilejowane konto jest faktycznie potrzebne i używane zgodnie z Twoim zasadami. Dostęp do danych kontroluj nie tylko w przypadku ludzi, ale i usług, procesów. Zmień domyślne hasła i (o ile jest to możliwe) loginy do urządzeń. Zweryfikuj konieczność dostępności każdego urządzenia z internetu (spoza sieci lokalnej). Jeśli urządzenie musi być dostępne z internetu, ukryj je za firewallem i udostępnij na niestandardowym porcie. Nie zapominaj o urządzeniach mobilnych i publicznych usługach, tam też są dane które chronisz.

Kieruj się priorytetami - wyróżnij krytyczne zasoby, zapewnij rezerwę
To Ty wiesz, bez których danych Twój biznes się załamie. Wiesz również jak używasz te dane w swoich usługach. Zapewnij, że mają one priorytet gdy zarządzasz technologią używaną do ich przetwarzania. Rozważ, czy wiesz wystarczająco dużo na temat zabezpieczeń technologii. Zarówno oszczędności w zakresie umiejętności administratorów jak i sprawności infrastruktury czy oprogramowania mogą wygenerować niespodziewane koszty. Pamiętaj, że każda technologia może być zawodna, lub zwyczajnie się zepsuć, dlatego zapewnij rozsądne rezerwy zarówno finansowe jak i "ludzkie" aby ograniczyć przestoje. Ucz się na błędach innych i nie balansuj na krawędzi pojemności, czy wydajności technologii. Mały błąd konfiguracji, atak odmowy usługi, czy zwykły wzrost zapotrzebowani na nią może kosztować Cię więcej niż się spodziewasz.

Pamiętaj o odpowiedzialności – zaplanuj i optymalizuj budżet, zachowaj zgodność z wymogami prawnymi

Technologia otwiera nowe możliwości, z którymi zawsze związany jest koszt. Wydatki związane z technologią to nie tylko zakup ale i utrzymanie danej technologii, oraz nierzadko jej zmiana na inną. Należy świadomie oszacować koszty związane z infrastrukturą, licencjami oprogramowania, usługami wdrożenia i utrzymania. Popularyzacja outsourcingu, kolokacji i usług chmurowych pozwala racjonalnie zarządzać kosztami stosując model satysfakcjonujący zarówno wymogi prawne (np. centrum przetwarzania danych), jak i elastyczność dostarczanych usług (np. multiplatformowość). Często licencja dla wybranej technologii nie obejmuje kosztów komponentów zależnych, które trzeba dodatkowo zakupić (bazy danych, pluginy). Konieczne jest również zwrócenie uwagi na elementy "open source" oraz "free software" które mogą przestać być wspierane lub mogą wprowadzić dodatkowe ryzyko podatności. W przypadku tworzenia własnego kodu, warto zadbać o zgodne z prawem przeniesienie praw własności do kodu na Twoją firmę.

Przede wszystkim to, co jest możliwe - używaj ekosystemu usług, zabezpiecz swoje interesy przy współpracy z innymi

Konkretna konfiguracja i wdrożenie różnych technologii może znacznie ograniczyć ich bazowe możliwości. Zanim zakupisz nową technologię, czy zmodernizujesz starą, przeprowadź analizę zysków i wpływu na oferowane usługi. Jeśli nie masz własnych zasobów, użyj usług firm zewnętrznych dokładnie precyzując co jest Twoim celem. Kiedykolwiek zaangażujesz zewnętrznego usługodawcę, zapewnij, że właściwe postanowienia prawne zostały zawarte, szczególnie te, dotyczące klauzuli poufności oraz dostępu i prawa do usunięcia danych przetwarzanych przez firmę trzecią na Twoje zlecenie. Zapewnij sobie również prawo do audytu zabezpieczeń zastosowanych do ochrony powierzonych danych. Jeśli przetwarzasz dane innych podmiotów, upewnij się, że robisz to zgodnie z prawem (np. posiadając właściwe zgody, cel i środki zabezpieczeń).

Jak nie Ty, to kto? - stosuj standardy technologiczne, zapewnij zgodność z wymogami rynku przez niezależne audyty

Nowoczesne technologie używane w biznesie coraz częściej podlegają standaryzacji, z jednej strony technicznej, z drugiej prawnej w zakresie ich zastosowania. Inwestycja w technologie, posiadające certyfikację, spełniające rozpoznawalne standardy nie tylko ułatwia ich wdrożenie, użycie i utrzymanie, może być również przydatne przy audytach, certyfikacjach i kontrolach dotyczących Twojego biznesu wymaganych prawem jak i oczekiwanych przez Twojego klienta. Budowanie biznesu w oparciu o przestarzałe, nie wspierane technologie nie tylko zwiększa ryzyko wystąpienia poważnego incydentu

bezpieczeństwa czy stabilności usług, może również narazić Twoją firmę na straty reputacyjne i kary regulatora Twojego rynku.

Obecnie, coraz więcej rynków używających technologii informatycznych wymaga szyfrowania danych zarówno w transporcie jak i spoczynku. Sprostanie temu wyzwaniu, szczególnie w zakresie ochrony danych pomiędzy odbiorcami Twoich usług (end-to-end), może wymagać starannego doboru technologii i utwardzenia jej konfiguracji, potwierdzone przez niezależny, zewnętrzny audyt. Pamiętaj, że fakt, nie spełnienia wymogów przez innych uczestników rynku nie jest wymówką, a raczej szansą na uzyskanie przewagi nad konkurencją.