RODO w IT, czyli audyt cyberbezpieczeństwa według ENISA

ENISA, czyli Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ang. The European Union Agency for Cybersecurity) niedawno opublikowała poradnik o tym, jak w 12 krokach zabezpieczyć organizację pod kątem cyberbezpieczeństwa. Przewodnik dedykowany jest małym i średnim przedsiębiorstwom. To właśnie przedstawicieli MŚP oraz niedużych instytucji szczególnie zachęcam do lektury.

Każde z zaleceń ENISA skonfrontowaliśmy z praktyką i doświadczeniami własnymi i naszych klientów. Na koniec przygotowaliśmy dla Ciebie checklistę, która może posłużyć za narzędzie prostego audytu IT Security w Twojej organizacji. Wszystko opisaliśmy w prosty i zrozumiały sposób. Nawet jeśli nie posiadasz zaawansowanej wiedzy informatycznej, będziesz w stanie podjąć konkretne działania.

Czy warto? To pytanie retoryczne. CSIS i McAfee oszacowały, że globalne straty spowodowane działalnością hakerów wyniosły w roku 2014 około 400 mld dolarów. W 2020 szkody szacowano już na blisko 1 bln dolarów! Te koszty to oczywiście nie tylko koszt zapłaconych okupów czy wartość utraconych danych. Jeśli zdarzy Ci się poważny incydent cyberbezpieczeństwa, poświęcisz dużo roboczogodzin na rozmowy z Zespołem i powrót do normalnego funkcjonowania. Twoja produkcja czy sprzedaż usług może się zatrzymać. Być może utracisz znaczące korzyści w postaci potencjalnych zleceń. W kryzysowe zarządzanie całą sytuacją zaangażowane będą kluczowe osoby w firmie.

Obszar zabezpieczeń IT jest również dokładnie analizowany przez UODO. Najwyższa i jedna z najwyższy kar nałożonych przez UODO, to kary nałożone właśnie za niewłaściwe zabezpieczenia IT Security. Kary, o których mowa to Morele.net oraz Virgin Mobile Polska.

Krok 1. Rozwijaj kulturę cyberbezpieczeństwa

Punkt jest bardzo ogólny. ENISA proponuje jednak kilka konkretnych działań. W szczególności chodzi o:

a. podział odpowiedzialności, powołanie osoby odpowiedzialnej za obszar cyberbezpieczeństwa,

b. audyty IT Security,

c. polityki cyberbezpieczeństwa.

Podział odpowiedzialności

Brak powołania osoby odpowiedzialnej za IT Security to bolączka nie tylko sektora MŚP. Również wiele dużych przedsiębiorstw nie wyznacza osób odpowiedzialnych za cyberbezpieczeństwo. Ktoś

jednak musi wziąć odpowiedzialność za zabezpieczenia IT. Wzięcie odpowiedzialności za obszar, nie oznacza, że taka osoba samodzielnie wykona wszystkie zadania. Jeśli wykonuję audyt w organizacji, w której nikt nie odpowiada za zabezpieczenia teleinformatyczne, to spodziewam się dużych braków i zaniedbań. Nawet jeśli Twoja organizacja jest niewielka, możesz podjąć pewne działania zabezpieczające.

Nie musisz zatrudniać kosztownego specjalisty IT Security. Obecnie na rynku działa dużo małych firm IT, które oferują wsparcie w tym zakresie. Koszty takiego wsparcia nie są już barierą nie do przeskoczenia dla większości firm sektora MŚP. Zewnętrzny dostawca może pomóc Ci lepiej zabezpieczyć się pod względem IT Security. Jeśli posiadasz podstawowy zakres wiedzy informatycznej, będziesz w stanie wdrożyć większość z zabezpieczeń opisanych w tym artykule.

Jest jeszcze jeden ważny element w MŚP – kwestia relacji. W większości MŚP duża część bieżących zadań jest wykonywana przez właścicieli firm osobiście. Wspólne ustalenie, kto odpowiada za działkę IT Security, pomoże relacjom wewnątrz Twojej organizacji i zapobiegnie wielu nieporozumieniom.

Audyty cyberbezpieczeństwa

Audyty cyberbezpieczeństwa brzmią jak duże i skomplikowane wyzwanie. Sprawdź naszą checklistę i przekonaj się, że nie jest to prawdziwa teza. Takie działania wcale nie muszą być trudne i niewykonalne dla przeciętnego przedsiębiorcy. Wypełnienie naszej checklisty możesz potraktować jako formę podstawowego audytu IT Security. Pamiętaj tylko o tym, że checklista jest dedykowana MŚP i niewielkim instytucjom, a nie dużym korporacjom. Również MŚP operujące na bardzo dużej ilości systemów, profilujące czy przetwarzające dane osobowe w bardzo skomplikowany sposób, będą wymagały bardziej złożonych i rozbudowanych działań.

Polityki cyberbezpieczeństwa

Polityka cyberbezpieczeństwa podobnie jak audyt kojarzy się z bardzo złożonym i skomplikowanym dokumentem. Nie musi takim być. Stosowane zabezpieczenia mogą zostać opisane w prosty i zrozumiały sposób. To samo tyczy się zaleceń dla Twoich współpracowników.

Na dobrą kulturę w obszarze IT Security składa się również reagowanie na błędy czy odstępstwa od procedur. Nie możesz wdrożyć zabezpieczeń i procedur, których potem nie będziesz sprawdzać. Wdrożenie procedury nie jest punktowym działaniem, polegającym na ogłoszeniu polityki. Polityka powinna być wytłumaczona, np. w formie krótkiego treningu. Po jakimś czasie trzeba sprawdzić, czy jest stosowana w praktyce.

Krok 2. Zapewnij szkolenia

Wiele razy pisaliśmy już na naszym blogu o tym, jak istotny jest obszar budowania świadomości. Bez odpowiedniego poziomu świadomości Zespołu żadne zabezpieczenia nie będą wystarczające. Trening musi być odpowiednio dopasowany do potrzeb Twojej organizacji. Musisz umieć odpowiedzieć np. na pytanie dlaczego te czy inne zabezpieczenia są potrzebne.

W przypadku wielu zabezpieczeń, potrzebne będzie więcej pracy dla Twoich pracowników. Na przykład stosowanie dodatkowego składnika uwierzytelniającego (2FA) czy bardziej skomplikowanego hasła w procesie logowania użytkownika. Żeby pracownicy przyswoili sobie nowe procedury, powinni wiedzieć, dlaczego Twój wybór padł na takie czy inne rozwiązania.

Krok 3. Zadbaj o dostawców i strony trzecie

ENISA mówi również o kontroli nad Twoimi dostawcami. Bardzo często przetwarzają oni dane osobowe w formie elektronicznej. Jeśli powierzasz swoje dane osobowe zewnętrznej firmie, pamiętaj o tym, że ona również może być przedmiotem ataku hakerów.

Wszyscy dostawcy, a w szczególności ci, którzy mają dostęp do wrażliwych informacji i/lub systemów powinni dawać gwarancję zapewnienia odpowiedniego poziomu bezpieczeństwa. Taką gwarancję możesz uzyskać poprzez:

a. odpowiednie postanowienia umowy powierzenia przetwarzania danych osobowych,

b. audyt procesora.

Kilka razy zdarzyła się nam sytuacja, kiedy dostawca (procesor), naraził na szkodę naszego klienta. Pierwszym co sprawdzamy w takiej sytuacji jest to, czy mamy umowę powierzenia. Dobra umowa powierzenia to już połowa sukcesu. Druga połowa to audytowanie przynajmniej części naszych dostawców. O audycie procesora pisaliśmy już na naszym blogu To nie jest skomplikowane działanie (w najprostszej wersji wystarczy checklista), a może Ci bardzo pomóc w krytycznej sytuacji. Dla sektora MŚP rekomenduję audytowanie kluczowych dostawców.

Krok 4. Plan reagowania na incydenty

Procedura reagowania na incydenty ochrony danych osobowych, to jedna z kluczowych procedur RODO, które wdrażamy. Im większa jest organizacja, tym trudniej zapewnić szybką reakcję na naruszenie.

Procedura dla MŚP może być bardzo prosta. Najważniejsze jest to, żeby wszystkie osoby odpowiedzialne za podjęcie decyzji, wiedziały co mają robić. W tym miejscu znów wraca temat osoby odpowiedzialnej za IT Security. Taka osoba musi być w stanie oszacować rozmiary incydentu i potencjalne zagrożenia od strony informatycznej. Ktoś powinien również wykonać analizę ryzyka dla incydentu i podjąć ostateczną decyzję o tym czy zgłaszamy go do UODO czy nie.

Sprawdź, czy wiesz kto i co powinien zrobić w sytuacji incydentu. Jeśli nie wiesz tego teraz, to w sytuacji naruszenia tym bardziej trudno będzie Ci podjąć odpowiednią decyzję.

Krok 5. Zabezpiecz dostępy hasłami

W tym zakresie ENISA zwraca szczególną uwagę na:

a. odpowiednią składnię,

b. używanie managerów haseł.

Temat polityki haseł to jeden z *must have* każdej organizacji. Problem w tym, że temat jest już tak wyeksploatowany, że wiele osób przestało przywiązywać do niego większą wagę. Problemem jest też to, że wiele organizacji stosuje sprzeczne ze sobą polityki haseł o różnym poziomie skomplikowania.

W kwestii zarządzania hasłami bardzo pomocne jest korzystanie z managerów haseł, takich jak np. KeePass. Przy obecnej liczbie haseł z których korzystamy, nie ma szans na ich zapamiętanie. W obecnych realiach podobne programy są skutecznym rozwiązaniem, które warto wdrożyć także w życiu prywatnym.

Krok 6. Zabezpiecz urządzenia

Na ten krok składają się między innymi:

a. aktualizowany software,

b. antywirus,

c. szyfrowanie,

d. stosowanie rozwiązań blokujących phishing i inny spam mailowy.

Brak aktualizacji oprogramowania to jeden z najczęstszych powodów wielu incydentów. Musisz wyrobić w sobie nawyk aktualizowania oprogramowania. Twój Zespół również musi posiadać taki nawyk.

Zwracam również uwagę na szyfrowanie. Zaszyfrowanie np. dysków twardych może być bardzo pomocne w przypadku kradzieży sprzętu. Znamy przypadek, gdzie kilka lat temu, zaszyfrowane dyski pomogły organizacji. Włamanie do biura zakończyło się kradzieżą kilku laptopów. Część z nich udało się odzyskać dlatego, że lombardy, w których złodziej chciał je upłynnić, odmawiały ich przyjęcia.

Jest jeszcze jedna dodatkowa korzyść z szyfrowania dysków twardych. Jeśli taki dysk zostanie skradziony, to szansa na to, że dane osobowe trafią w niepowołane ręce jest minimalna. Wielokrotnie zaszyfrowane dyski twarde ratowały naszych klientów przed koniecznością zgłaszania incydentów do Urzędu Ochrony Danych Osobowych. Zaszyfrowanie dysku twardego to dość prosta operacja, jeśli jednak nie posiadasz pewnego zasobu wiedzy IT, warto będzie skorzystać z pomocy specjalisty.

Krok 7. Zabezpiecz swoją sieć

Chodzi między innymi o:

a. zarządzanie laptopami i urządzeniami mobilnymi,

b. stosowanie firewalla,

c. bieżącą aktualizację procedur i zabezpieczeń zdalnego dostępu.

W dobie powszechnie stosowanej pracy zdalnej pamiętaj o odpowiednim zabezpieczeniu laptopów Twoich pracowników. Jeśli pracują na własnych urządzeniach, nie zapomnij o ustaleniu i wdrożeniu konkretnych zasad takiej pracy.

Przede wszystkim kluczowe będzie zorganizowanie backupów. Mogą się one tworzyć zdalnie lub ich utworzenie będzie wymagało wizyty w biurze.

Jeśli do pracy Twojemu zespołowi niezbędny jest dostęp do zasobów sieciowych, zastanów się koniecznie nad stosowaniem VPNów. Konfiguracja bezpiecznego połączenia VPN może również wymagać nieco bardziej specjalistycznej wiedzy z zakresu IT.

Krok 8. Podwyższaj i monitoruj zabezpieczenia fizyczne

Na cyberbezpieczeństwo ma również wpływ obszar zabezpieczeń fizycznych. W jaki sposób zabezpieczona jest Twoja serwerownia? Gdzie odkładasz laptopy po zakończonym dniu pracy? Gdzie odkładają je Twoi pracownicy? Zabezpieczenia fizyczne również grają istotną rolę dla ryzyka naruszenia Twoich danych. Mimo, że fizyczna kradzież sprzętu jest mniej prawdopodobna niż kiedyś, to jednak wciąż się może zdarzyć.

Krok 9. Zabezpiecz backupy

Zagwarantuj, że backupy w Twojej organizacji:

a. tworzone są regularnie,

b. przechowywane są gdzie indziej niż bieżące dane.

Firma Veaam szacuje, że nawet 58% prób przywrócenia danych z backupów kończy się niepowodzeniem. Znamy to z autopsji. Kilkukrotnie naszym klientom zdarzyło mi się stracić cenne dane (nie tylko osobowe, ale i biznesowe) i mimo, że teoretycznie backupy były tworzone, to w

praktyce nie udało się odzyskać kompletu informacji. Procedura backupów automatycznych często jest dość skomplikowana. Na jej skuteczność może mieć wpływ wiele różnych czynników. Dlatego warto co jakiś czas sprawdzić, czy backupy faktycznie są tworzone.

Kolejny fundament bezpiecznego przechowywania danych, to umiejscowienie backupów w innej lokalizacji niż dane przetwarzane „na bieżąco". Jeśli przechowujesz kopie zapasowe w tym samym pokoju, w którym znajduje się Twój komputer z backupowanymi danymi, to w przypadku pożaru czy włamania tracisz wszystkie dane. Procedury backupowe mają ograniczony sens, jeśli trzymasz dane w tym samym miejscu co kopie zapasowe.

Krok 10. Stosuj świadomie rozwiązania chmurowe

Zagrożenia i szanse wynikające z korzystania z chmury obliczeniowej mogą być bardzo różne dla różnych organizacji. Wiele w tym zakresie zależy od rodzaju chmury, rodzaju przetwarzanych w niej informacji oraz procesów, których to przetwarzanie dotyczy.

Korzystanie z chmury powinno być w pełni świadome, a w szczególności świadomy powinien być wybór dostawcy usługi. Dobry dostawca powinien być w stanie zrealizować nasze rzeczywiste potrzeby, gwarantując przy tym bezpieczeństwo przechowywanych danych.

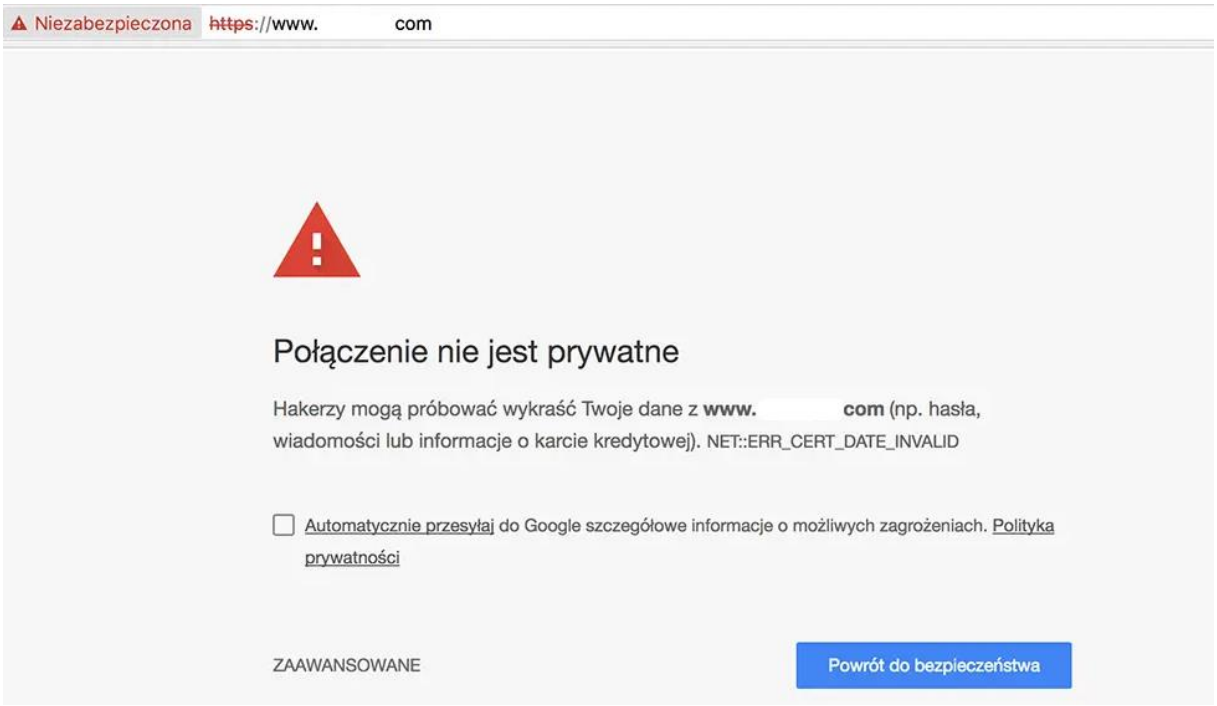
W kontekście ochrony danych osobowych powinniśmy szukać podmiotu, który zagwarantuje przestrzeganie przepisów RODO, w szczególności, jeżeli dane przechowywane będą poza UE/EOG.

Wiele cennych wskazówek w tym zakresie zawiera wydany przez ENISA Przewodnik dotyczący bezpieczeństwa w chmurze dla MŚP.

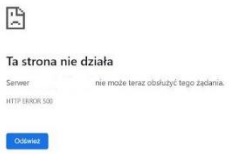
Krok 11. Zabezpiecz swoje strony www

Jeśli na Twojej stronie internetowej znajdują się dane szczególnych kategorii, dane płatnicze etc., to zdecydowanie warto zadbać w sposób szczególny o ich bezpieczeństwo. Bezwzględnie stosuj certyfikaty SSL zabezpieczające poufność danych przekazywanych przez użytkownika. Nie wiąże się to z dużym wydatkiem finansowym, a znacznie zwiększy bezpieczeństwo Twoich klientów.

Do tego dochodzą jeszcze straty wizerunkowe. Chyba nie chcesz, żeby Twój klient po wejściu na Twoją stronę internetową zobaczył coś takiego:



Co jeszcze warto wdrożyć? Zabezpieczyć dostęp do systemu do zarządzania treścią na stronie internetowej (CMS). Jeśli korzystasz np. z systemu WordPress – zainstaluj lub zakup odpowiednie oprogramowanie antywirusowe i firewall zabezpieczające przed atakami z zewnątrz. Ograniczy to nie tylko ryzyko niekontrolowanego dostępu do firmowych danych, ale skutecznie wyeliminuje też podejrzane wejścia na Twoją stronę internetową. Jeśli w porę tego nie zrobisz, któregoś dnia Twój przeciążony serwer może odmówić Ci posłuszeństwa, a Twój klient zobaczy coś takiego:



Na bieżąco monitoruj i kontroluj dostępy do swojej strony www oraz serwera FTP. Może część z nich powinna zostać wycofana? Może jakieś uprawnienie dla zewnętrznego dostawcy zostało nadane zbyt szeroko? A może warto dodać kolejny składnik uwierzytelniający (2FA) do procesu logowania do Twojego CMSa?

Krok 12. Dziel się informacjami o cyberbezpieczeństwie z innymi

Wyzwaniem dla MŚP jest dostępność i przydatność wytycznych w postaci norm, białych ksiąg lub innych podobnych materiałów. Oczywiście istnieją dokumenty poświęcone cyberbezpieczeństwu, jednak większość z nich albo zawiera ogólne informacje, albo odnosi się do większych organizacji z funkcjonującymi od lat ramami cyberbezpieczeństwa.

Dlatego też, informacje o nowych formach ataków czy zagrożeń warto wymieniać w obrębie własnej organizacji i nie tylko. To również element budowania kultury cyberbezpieczeństwa.

Podsumowanie

Większość przedsiębiorstw MŚP jest znacząco limitowana czasem i ograniczonym budżetem. Brakuje kadr i zasobów, które ułatwią wykonanie audytu IT. Przedsiębiorcy wyobrażają sobie, że zadbanie o ten obszar to ogromny koszt i wielkie wyzwanie.

W praktyce zbadanie podstaw obszaru cyberbezpieczeństwa, nie musi być trudne, drogie i czasochłonne. Pierwszy krok w zakresie budowy wysokiej jakości zabezpieczeń, może być wykonany w prosty i szybki sposób. Skorzystaj z naszej checklisty i stopniowo rozbudowuj swoje zabezpieczenia.

Autor artykułu:

Przemysław Zegarek

Źródła:

- Przewodnik po cyberbezpieczeństwie dla MŚP — 12 kroków do zabezpieczenia Twojej firmy
- Cyberbezpieczeństwo dla MŚP – wyzwania i zalecenia
- Przewodnik dotyczący bezpieczeństwa w chmurze dla MŚP