AGENCJA UNII EUROPEJSKIEJ
DS. CYBERBEZPIECZEŃSTWA

Przewodnik po cyberbezpieczeństwie dla MŚP

12 KROKÓW

DZIĘKI KTÓRYM ZABEZPIECZYSZ SWOJĄ FIRMĘ

Kryzys zapoczątkowany przez pandemię COVID-19 doskonale uwidocznił znaczenie komputerów i Internetu dla firm z sektora małych i średnich przedsiębiorstw (MŚP). By zadbać o rozwój swoich przedsięwzięć w czasie pandemii, wiele firm musiało podjąć działania ukierunkowane na zapewnienie ciągłości działalności, obejmujące między innymi integrację usług w chmurze, znalezienie nowych dostawców usług internetowych, aktualizację stron internetowych i umożliwienie pracownikom pracy zdalnej.

W poradniku znajdziesz wskazówki, dzięki którym dowiesz się, jak lepiej zabezpieczyć swoje systemy i firmę. Ta publikacja towarzyszy bardziej szczegółowemu sprawozdaniu – „**Cyberbezpieczeństwo dla MŚP – Wyzwania i zalecenia**" (Cybersecurity for SMES – Challenges and recommendations) wydanemu przez agencję ENISA.

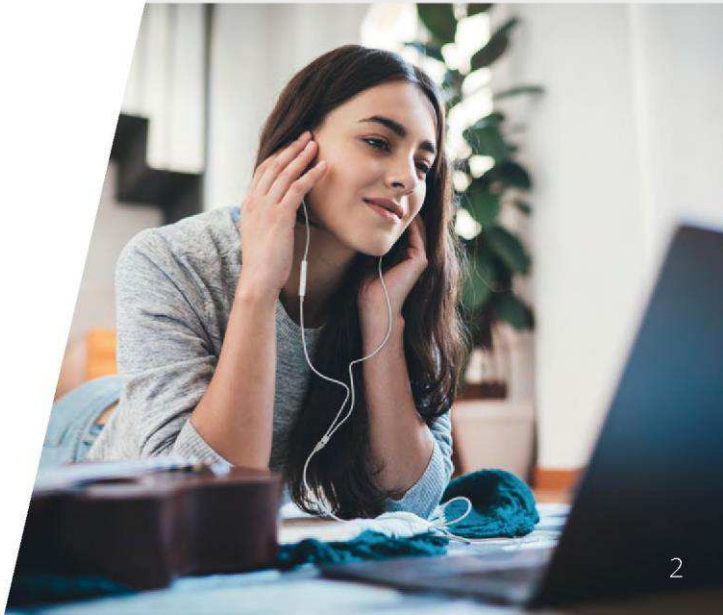
1 BUDUJ KULTURĘ CYBERBEZPIECZEŃSTWA

WYZNACZ OSOBY ODPOWIEDZIALNE ZA ZARZĄDZANIE

Dbałość o cyberbezpieczeństwo jest kluczem do sukcesu każdej firmy z sektora MŚP. Odpowiedzialność za ten kluczowy obszar powinna ponosić wyznaczona w organizacji osoba. Jej zadania? Dbałość o to, by kwestie związane z cyberbezpieczeństwem były brane pod uwagę w procesie planowania czasu pracowników, zakupu oprogramowania, usług i sprzętu zabezpieczającego, a także oferowania szkoleń dla pracowników czy wdrażania skutecznych zasad.

ZADBAJ O ZAANGAŻOWANIE PRACOWNIKÓW

Zadbanie o zaangażowanie pracowników to klucz do skutecznego wdrożenia zasad. Jak to zrobić? Pomogą skuteczna komunikacja na temat zagadnień związanych z cyberbezpieczeństwem, otwarte poparcie - ze strony kierownictwa - dla inicjatyw w tym zakresie, szkolenia dla pracowników oraz zapewnienie zespołowi jasnych i konkretnych zasad określonych w polityce cyberbezpieczeństwa.



OPUBLIKUJ REGULAMINY CYBERBEZPIECZEŃSTWA

Regulaminy cyberbezpieczeństwa powinny zawierać jasne i konkretne zasady dla pracowników dotyczące korzystania ze środowisk, sprzętu i usług informacyjno-komunikacyjnych w firmie. Zasady te powinny również określać konsekwencje, jakie mogą spotkać pracownika w przypadku nieprzestrzegania tych zasad.
Pamiętaj o regularnym przeglądzie i aktualizacji regulaminów!

PRZEPROWADŹ AUDYT CYBERBEZPIECZEŃSTWA

Regularne audyty powinny być przeprowadzane przez osoby mające odpowiednią wiedzę, umiejętności i doświadczenie. Audytorzy powinni być niezależni, bez względu na to, czy są to wykonawcy zewnętrzni czy też pracownicy wewnętrzni. Audytorzy nie powinni być odpowiedzialni za codzienną obsługę działu IT firmy.

PAMIĘTAJ O OCHRONIE DANYCH

Zgodnie z ogólnym rozporządzeniem UE o ochronie danych[1] wszystkie MŚP przetwarzające lub przechowujące dane osobowe należące do mieszkańców UE/EOG muszą zapewnić odpowiednie środki bezpieczeństwa w celu ochrony tych danych. Obejmuje to zapewnienie, że wszelkie podmioty zewnętrzne działające w imieniu i na zlecenie MŚP wdrożyły odpowiednie środki bezpieczeństwa.

1. Ogólne rozporządzenie o ochronie danych osobowych (RODO) https://ec.europa.eu/info/law/law-topic/data-protection_pl

2

ZADBAJ O ODPOWIEDNIE SZKOLENIA

Zadbaj o regularne szkolenia pracowników zwiększające świadomość cyberzagrożeń. To ważne, by potrafili je rozpoznać i radzić sobie z nimi. Szkolenia powinny być dostosowane do potrzeb firmy i koncentrować się na realistycznych scenariuszach.

Zapewnienie specjalistycznych szkoleń z zakresu cyberbezpieczeństwa dla osób odpowiedzialnych za zarządzanie tym obszarem w przedsiębiorstwie pozwoli im na zbudowanie umiejętności i kompetencji wymaganych do skutecznego wykonywania swoich zadań.

3

ZADBAJ O BEZPIECZEŃSTWO PODMIOTÓW ZEWNĘTRZNYCH

Wszyscy kontrahenci firmy, szczególnie posiadający dostęp do wrażliwych danych lub kluczowych systemów, powinni spełniać uzgodnione poziomy bezpieczeństwa. Zadbaj o to! Równie ważne jest zawarcie umów regulujących spełnianie wymogów bezpieczeństwa przez dostawców i kontrahentów.

4

OPRACUJ PLAN REAGOWANIA NA INCYDENTY

Opracuj formalny plan reagowania na incydenty, który będzie zawierał jasne wytyczne, udokumentowane role i obowiązki. Celem takiego planu jest zapewnienie profesjonalnej, sprawnej i szybkiej reakcji na wszystkie incydenty związane z bezpieczeństwem. Aby szybko reagować na zagrożenia, warto wdrożyć narzędzia, które pozwalają na monitorowanie infrastruktury i alarmowanie w przypadku wystąpienia podejrzanej aktywności lub naruszenia bezpieczeństwa

5 ZABEZPIECZ DOSTĘP DO SYSTEMÓW

Zachęcaj wszystkich do używania haseł opartych na co najmniej trzech losowych słowach połączonych we frazę. Takie rozwiązanie przy tworzeniu hasła stanowi bardzo dobre połączenie łatwości zapamiętywania i bezpieczeństwa.

Jeśli postawisz na typowe hasła:

- Powinny być długie, obejmować małe i wielkie litery, a także cyfry i znaki specjalne.
- Nie powinny być oczywiste, tak jak na przykład „haslo123". Warto unikać także ciągów liter („abc") lub cyfr („123").
- Nie powinny obejmować danych osobowych, które można znaleźć w Internecie.

Niezależnie od tego, który wariant hasła zastosujesz:

- W każdym serwisie internetowycm korzystaj z innego hasła!
- Nie udostępniaj swoich haseł innym osobom.
- Włącz uwierzytelnianie wieloskładnikowe.
- Używaj menedżera haseł.

****

6

ZABEZPIECZ URZĄDZENIA

Zapewnienie bezpieczeństwa urządzeń, z których korzystają pracownicy – komputerów stacjonarnych, laptopów, tabletów czy smartfonów – jest kluczowym krokiem w programie zapewniania cyberbezpieczeństwa.

AKTUALIZUJ OPROGRAMOWANIE

Najlepszym rozwiązaniem jest wykorzystanie scentralizowanej platformy do zarządzania poprawkami.
MŚP powinny przede wszystkim:

- Regularnie aktualizować oprogramowanie wykorzystywane w firmie.
- Włączyć automatyczne aktualizacje, jeśli tylko jest to możliwe.
- Określić urządzenia i oprogramowanie wymagające ręcznych aktualizacji.
- Pamiętaj także o aktualizacji urządzeń mobilnych i IoT.

PAMIĘTAJ O ANTYWIRUSIE

Centralnie zarządzane rozwiązanie antywirusowe powinno być wdrożone na wszystkich urządzeniach i regularnie aktualizowane w celu zapewnienia ciągłej i skutecznej ochrony.
Korzystaj tylko z legalnego oprogramowania!

CHROŃ POCZTĘ ELEKTRONICZNĄ

Stosuj rozwiązania blokujące spam, wiadomości zawierające odnośniki do złośliwych witryn, złośliwe załączniki, w tym wirusy, a także phishing.

SZYFRUJ DANE

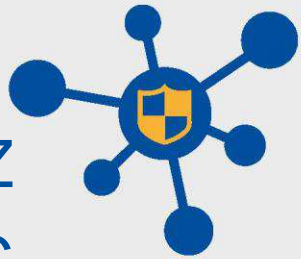
Chroń dane poprzez ich zaszyfrowanie.
MŚP powinny zadbać o szyfrowanie danych przechowywanych na urządzeniach przenośnych, takich jak laptopy, smartfony i tablety. W przypadku danych przesyłanych za pośrednictwem sieci publicznych, takich jak hotelowe lub lotniskowe sieci Wi-Fi, należy upewnić się, że dane są zaszyfrowane.
Jak to zrobić? Wystarczy VPN - wirtualnej sieci prywatnej lub korzystanie wyłącznie ze stron opartych na protokole SSL/TLS. Upewnij się, że strony internetowe, z których korzystasz do przesyłania danych wykorzystują odpowiednią technologię szyfrowania.

DBAJ O URZĄDZENIA MOBILNE

Ułatwiając pracownikom pracę zdalną wiele firm pozwala im na korzystanie z własnych laptopów, tabletów bądź smartfonów. Prowadzi to do wielu obaw dotyczących bezpieczeństwa wrażliwych danych biznesowych przechowywanych na tych urządzeniach. Jednym ze sposobów zarządzania tym ryzykiem jest zastosowanie rozwiązania do zarządzania urządzeniami mobilnymi (Mobile Device Management, MDM), które pozwala MŚP na:

- Kontrolę, jakie urządzenia mają dostęp do systemów i usług.
- Zapewnienie, że na urządzeniu jest zainstalowane aktualne oprogramowanie antywirusowe.
- Ustalenie, czy dane urządzenie jest zaszyfrowane.
- Potwierdzenie, czy urządzenie ma zainstalowane aktualne poprawki bezpieczeństwa.
- Wymuszenie ochrony urządzenia kodem PIN lub hasłem.
- Zdalne wymazanie wszelkich danych firmy z urządzenia, jeśli właściciel zgłosi jego zagubienie lub kradzież, a także w przypadku rozwiązania stosunku pracy.

7 ZABEZPIECZ SWOJĄ SIEĆ



STOSUJ ZAPORY OGNIOWE

Zapory ogniowe (ang. firewall) kontrolują przychodzący i wychodzący ruch sieciowy, dzięki czemu są kluczowym narzędziem pozwalającym na ochronę firmy. Powinny być skonfigurowane do ochrony wszystkich najważniejszych systemów w szczególności powinny chronić wewnętrzną sieć firmy przed dostępem z Internetu.

SPRAWDŹ ROZWIĄZANIA ZDALNEGO DOSTĘPU

Firmy powinny regularnie sprawdzać wszelkie narzędzia zdalnego dostępu, aby zapewnić ich bezpieczeństwo.

- Upewnij się, że oprogramowanie wykorzystywane do zdalnego dostępu jest aktualne i ma zainstalowane najnowsze poprawki bezpieczeństwa.
- Ogranicz dostęp zdalny z podejrzanych lokalizacji geograficznych lub określonych adresów IP.
- Zapewnij pracownikom dostęp wyłącznie do systemów i komputerów, których potrzebują do pracy.
- Wymuszaj stosowanie silnych haseł i w miarę możliwości włączaj uwierzytelnianie wieloskładnikowe.
- Włącz rozwiązania monitorujące i alarmy, aby otrzymywać informacje na temat potencjalnych ataków oraz podejrzanej aktywności.

8 ZWIĘKSZ BEZPIECZEŃSTWO FIZYCZNE

Wszędzie tam, gdzie znajdują się ważne dane, należy stosować odpowiednie zabezpieczenia fizyczne. Nie pozostawiaj firmowych urządzeń bez opieki, czy na tylnym siedzeniu samochodu. Każde odejście od komputera powinno się wiązać z jego zablokowaniem, można także włączyć funkcję automatycznego blokowania na każdym urządzeniu używanym do celów służbowych. Nie należy pozostawiać wrażliwych dokumentów bez nadzoru, a gdy nie są potrzebne, należy zadbać o ich bezpieczne przechowywanie.

9 ZADBAJ O KOPIE ZAPASOWE

Aby umożliwić odzyskanie kluczowych danych, zadbaj o kopie zapasowe, które są skutecznym sposobem na przywrócenie systemów po incydentach takich jak atak ransomware. Stosuj następujące zasady tworzenia kopii zapasowych:

- Kopie zapasowe powinny być regularne i w miarę możliwości zautomatyzowane.
- Kopie nie powinny być połączone ze środowiskiem produkcyjnym firmy.
- Kopie powinny być szyfrowane, zwłaszcza w przypadku przenoszenia ich między biurami.
- Kopie należy regularnie testować pod kątem odzyskiwania danych. Warto przeprowadzać regularne testy kompleksowego przywracania systemów i danych.

10

KORZYSTAJ Z CHMURY

Rozwiązania oparte na chmurze oferują wiele korzyści, jednak przed nawiązaniem współpracy z dostawcą usług w chmurze warto również wziąć pod uwagę zagrożenia. Agencja ENISA opublikowała Przewodnik dla MŚP dotyczący bezpieczeństwa w chmurze[2], z którym warto się zapoznać w przypadku chęci migracji do chmury.

Wybierając dostawcę usług chmurowych, firmy powinny upewnić się, że nie narusza on żadnych praw lub regulacji poprzez przechowywanie danych – w szczególności danych osobowych – poza terytorium UE/EOG. Przepisy RODO wymagają by dane osób zamieszkałych na terytorium UE/EOG nie były przechowywane ani przekazywane poza granice UE/EOG, z wyjątkiem szczególnych sytuacji, które wymagają specjalnych zasad.

2. https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 ZABEZPIECZ STRONY INTERNETOWE

Ważne jest zadbanie o prawidłową konfigurację i bezpieczeństwo stron internetowych firmy, a także o właściwą ochronę danych osobowych i informacji finansowych, w tym danych dotyczących kart kredytowych. Regularnie przeprowadzaj testy bezpieczeństwa stron internetowych w celu zidentyfikowania wszelkich potencjalnych luk bezpieczeństwa. Prowadź też regularne przeglądy, by sprawdzić czy strona jest utrzymywana i aktualizowana prawidłowo.

12 SZUKAJ INFORMACJI, ROZPOWSZECHNIAJ WIEDZĘ

Skutecznym narzędziem w walce z cyberprzestępczością jest rozpowszechnianie wiedzy. Wymiana informacji związanych z cyberprzestępczością ma kluczowe znaczenie dla MŚP. Pozwala im lepiej zrozumieć zagrożenia, na jakie są narażone.
Firmy, które - dzięki innym przedsiębiorcom - poznają zagrożenia i wyzwania, a także potencjalne rozwiązania - chętniej z nich skorzystają niż gdyby poznały je z branżowych sprawozdań lub wyników badań dotyczących cyberbezpieczeństwa.

AGENCJA UNII EUROPEJSKIEJ
DS. CYBERBEZPIECZEŃSTWA

ENISA – podstawowe informacje

ENISA, czyli Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, jest unijną agencją, której celem jest osiągnięcie i zapewnienie wysokiego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w 2004 roku instytucja, wzmocniona unijnym Aktem o Cyberbezpieczeństwie przyczynia się do realizacji unijnej polityki w zakresie cyberbezpieczeństwa, dba o wiarygodność produktów, usług i procesów TIK dzięki systemom certyfikacji cyberbezpieczeństwa, współpracuje z państwami członkowskimi i organami UE oraz pomaga Europie w przygotowaniu się do przyszłych wyzwań w tym zakresie. Agencja współpracuje z kluczowymi interesariuszami dzieląc się wiedzą, budując potencjał i podnosząc świadomość, by zwiększyć zaufanie do połączonej gospodarki, zadbać o bezpieczeństwo unijnej infrastruktury oraz zapewnić bezpieczeństwo cyfrowe mieszkańcom i obywatelom Europy. Więcej informacji można znaleźć na stronie www.enisa.europa.eu.

ENISA

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

Biuro w Atenach

Ethnikis Antistaseos 72 i

Agamemnonos 14,

Chalandri 15231, Attiki, Grecja

Biuro w Heraklionie

95 Nikolaou Plastira

700 13 Vassilika Vouton,

Heraklion, Grecja

enisa.europa.eu

Tłumaczenie:

GOV.pl CYFRYZACJA