AGENCJA UNII EUROPEJSKIEJ DS.
CYBERBEZPIECZEŃSTWA

Przewodnik po bezpieczeństwie cybernetycznym dla MŚP

12 KROKÓW

DO BEZPIECZEŃSTWA TWOJEJ FIRMY

Kryzys COVID-19 pokazał, jak ważne dla MŚP są internet i ogólnie rzecz biorąc komputery. Aby dobrze prosperować w biznesie podczas pandemii, wiele MŚP musiało podjąć środki zapewniające ciągłość biznesową, takie jak przejście na usługi w chmurze, poprawa usług internetowych, aktualizacja stron internetowych i umożliwienie pracownikom pracy zdalnej.

Niniejsza ulotka zawiera informacje o praktycznych 12 krokach wysokiego szczebla do lepszego zabezpieczenia systemów i interesów MŚP. Jest to publikacja towarzysząca bardziej szczegółowemu sprawozdaniu ENISA **„Cybersecurity for SMES – Challenges and Recommendations” („Cyberbezpieczeństwo dla MŚP: wyzwania i zalecenia”)**.

1 ROZWIJAJ DOBRĄ KULTURĘ CYBERBEZPIECZEŃSTWA

PRZYPISUJ ODPOWIEDZIALNOŚĆ ZA ZARZĄDZANIE

Dobre cyberbezpieczeństwo jest kluczowym elementem w ciągłym sukcesie każdego MŚP. Odpowiedzialność za tę kluczową funkcję należy przypisać takiej osobie w organizacji, która powinna zapewnić, że cyberbezpieczeństwu przydzielono odpowiednie zasoby, takie jak czas pracowników, zakup oprogramowania, usług i sprzętu do zapewnienia cyberbezpieczeństwa, szkolenia dla pracowników oraz opracowanie skutecznych polityk.

ZYSKAJ AKCEPTACJĘ PRACOWNIKÓW

Uzyskaj akceptację pracowników przez skuteczną komunikację na temat cyberbezpieczeństwa ze strony kierownictwa, otwarte wspieranie inicjatyw w zakresie cyberbezpieczeństwa przez kierownictwo, odpowiednie szkolenia dla pracowników oraz zapewnienie pracownikom jasnych i konkretnych zasad określonych w polityce cyberbezpieczeństwa.

PUBLIKUJ POLITYKĘ CYBERBEZPIECZEŃSTWA

W polityce cyberbezpieczeństwa należy określić jasne i konkretne zasady dla pracowników dotyczące tego, jak powinni się zachowywać podczas korzystania ze środowiska, sprzętu i usług ICT przedsiębiorstwa. Zasady te powinny również podkreślać konsekwencje, jakie mogą spotkać pracownika w przypadku nieprzestrzegania tych zasad. Politykę te należy regularnie poddawać przeglądowi i aktualizować.

PRZEPROWADZAJ AUDYTY CYBERBEZPIECZEŃSTWA

Regularne audyty powinny przeprowadzać osoby posiadające odpowiednią wiedzę, umiejętności i doświadczenie. Audytorzy powinni być niezależni, bez względu na to, czy są to wykonawcy zewnętrzni, czy też pracownicy wewnętrzni MŚP, oraz niezależni od codziennych operacji informatycznych.

PAMIĘTAJ O OCHRONIE DANYCH

Zgodnie z ogólnym rozporządzeniem UE o ochronie danych[1] wszystkie MŚP, które przetwarzają lub przechowują dane osobowe należące do mieszkańców UE/EOG, muszą zapewnić odpowiednie kontrole bezpieczeństwa w celu ochrony tych danych. Obejmuje to zapewnienie, że wszelkie osoby trzecie pracujące w imieniu MŚP dysponują odpowiednimi środkami bezpieczeństwa.

[1] Ogólne rozporządzenie o ochronie danych https://ec.europa.eu/info/law/law-topic/data-protection_pl

2

ORGANIZUJ ODPOWIEDNIE SZKOLENIA

Organizuj regularne szkolenia w zakresie świadomości na temat cyberbezpieczeństwa dla wszystkich pracowników w celu dopilnowania, aby potrafili oni rozpoznawać i radzić sobie z różnymi zagrożeniami dla cyberbezpieczeństwa. Szkolenia te powinny być dostosowane do potrzeb MŚP i koncentrować się na rzeczywistych sytuacjach życiowych.

Zapewniaj specjalistyczne szkolenia z zakresu cyberbezpieczeństwa dla osób odpowiedzialnych za zarządzanie cyberbezpieczeństwem w przedsiębiorstwie, aby zapewnić im umiejętności i kompetencje wymagane do wykonywania pracy.

3

ZAPEWNIJ SKUTECZNE ZARZĄDZANIE PODMIOTAMI ZEWNĘTRZNYMI

Zapewnij, by wszyscy dostawcy, w szczególności ci, którzy mają dostęp do wrażliwych danych lub systemów, byli aktywnie zarządzani i osiągali uzgodnione poziomy bezpieczeństwa. Należy zawrzeć umowy regulujące sposób, w jaki dostawcy spełniają te wymogi bezpieczeństwa.

4

OPRACUJ PLAN REAGOWANIA NA INCYDENTY

Opracowanie formalnego planu reagowania na incydenty, który zawiera jasne wytyczne, udokumentowane role i obowiązki, aby zapewnić, że wszystkie incydenty związane z bezpieczeństwem spotykają się z reakcją w sposób terminowy, profesjonalny i właściwy. Aby szybko reagować na zagrożenia dla bezpieczeństwa, należy zbadać narzędzia, które mogą monitorować i tworzyć alerty w przypadku wystąpienia podejrzanej aktywności lub naruszenia bezpieczeństwa.

5 ZABEZPIECZ DOSTĘP DO SYSTEMÓW

Zachęcaj wszystkich do używania hasła-frazy, czyli zbioru co najmniej trzech przypadkowych, popularnych słów połączonych we frazę, które stanowią bardzo dobre połączenie łatwości zapamiętywania i bezpieczeństwa. Jeśli zdecydujesz się na typowe hasło:

- niech będzie długie, z małymi i wielkimi literami, ewentualnie także cyframi i znakami specjalnymi,
- unikaj oczywistych fraz, takich jak „hasło”, ciągów liter lub cyfr, takich jak „abc”, liczb jak „123”,
- unikaj używania danych osobowych, które można znaleźć w internecie.

Niezależnie od tego, czy używasz haseł czy fraz,

- nie używaj ich ponownie w innych miejscach,
- nie udostępniaj ich współpracownikom,
- włącz uwierzytelnianie wieloskładnikowe,
- korzystaj z dostosowanego menedżera haseł.

6

ZABEZPIECZ URZĄDZENIA

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

REGULARNE ŁATANIE I AKTUALIZOWANIE OPROGRAMOWANIA

Idealnym rozwiązaniem jest użycie scentralizowanej platformy do zarządzania poprawkami [łatami] oprogramowania. Wysoce zalecane jest, aby MŚP:

- regularnie aktualizowały całe swoje oprogramowanie,
- w miarę możliwości włączały automatyczne aktualizacje,
- identyfikowały oprogramowanie i sprzęt, które wymagają ręcznych aktualizacji,
- uwzględniały urządzenia mobilne i internetu rzeczy.

ANTYWIRUS

Centralnie zarządzane rozwiązanie antywirusowe powinno być wdrożone na wszystkich typach urządzeń i aktualizowane w celu zapewnienia jego ciągłej skuteczności. Nie należy również instalować pirackiego oprogramowania, ponieważ może ono zawierać złośliwe oprogramowanie.

STOSUJ NARZĘDZIA OCHRONY POCZTY ELEKTRONICZNEJ I STRON INTERNETOWYCH

Stosuj rozwiązania w celu blokowania wiadomości spam, wiadomości zawierających linki do szkodliwych stron internetowych, wiadomości zawierających złośliwe załączniki (np. wirusy) i wiadomości służących wyłudzeniu informacji.

SZYFROWANIE

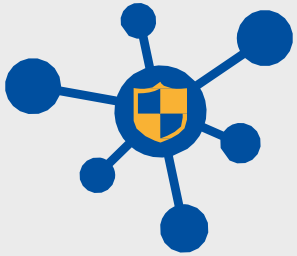
Chroń dane przez ich szyfrowanie. MŚP powinny zapewnić szyfrowanie danych przechowywanych na urządzeniach przenośnych, takich jak laptopy, smartfony i tablety. W przypadku danych przesyłanych za pośrednictwem sieci publicznych, takich jak hotelowe lub lotniskowe sieci WiFi, należy upewniać się, że dane są zaszyfrowane przy pomocy wirtualnej sieci prywatnej (VPN) lub uzyskiwać dostęp do witryn internetowych za pośrednictwem bezpiecznych połączeń z wykorzystaniem protokołu SSL/TLS. Należy upewniać się, że własne strony internetowe wykorzystują odpowiednią technologię szyfrowania w celu ochrony danych klienta podczas ich przesyłania przez internet.

WDRÓŻ ZARZĄDZANIE URZĄDZENIAMI MOBILNYMI

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

- kontrolować, jakie urządzenia mają dostęp do systemów i usług,
- zapewniać, że na urządzeniu zainstalowane jest aktualne oprogramowanie antywirusowe,
- ustalić, czy urządzenie jest zaszyfrowane,
- potwierdzić, czy urządzenie ma zainstalowane aktualne poprawki oprogramowania,
- egzekwować ochronę urządzenia kodem PIN lub hasłem,
- zdalnie wymazać wszelkie dane MŚP z urządzenia w przypadku zgłoszenia przez właściciela urządzenia jego zagubienia lub kradzieży, lub w przypadku zakończenia zatrudnienia właściciela urządzenia w danym MŚP.

7 ZABEZPIECZ SWOJĄ SIEĆ



STOSUJ ZAPORY SIECIOWE

Zapory sieciowe zarządzają ruchem wchodzącym do i wychodzącym z sieci i są kluczowym narzędziem w ochronie systemów MŚP. Zapory sieciowe powinny być rozmieszczone w celu ochrony wszystkich kluczowych systemów, w szczególności zaporę sieciową należy stosować do ochrony sieci MŚP przed internetem.

DOKONUJ PRZEGLĄDU ROZWIĄZAŃ ZDALNEGO DOSTĘPU

MŚP powinny regularnie sprawdzać wszelkie narzędzia zdalnego dostępu, aby zapewnić ich bezpieczeństwo, w szczególności:

- zapewniać, że całe oprogramowanie zdalnego dostępu jest poprawione i aktualne,
- ograniczać dostęp zdalny z podejrzanych położeń geograficznych lub określonych adresów IP,
- ograniczać zdalny dostęp pracowników tylko do tych systemów i komputerów, które są im potrzebne do pracy,
- egzekwować stosowanie silnych haseł przy dostępie zdalnym i w miarę możliwości włączać uwierzytelnianie wieloskładnikowe,
- zapewniać, że włączone jest monitorowanie i ostrzeganie o podejrzanych atakach lub nietypowej podejrzanej aktywności.

8 POPRAW BEZPIECZEŃSTWO FIZYCZNE

Wszędzie tam, gdzie znajdują się ważne informacje, należy stosować odpowiednie kontrole fizyczne. Na przykład firmowego laptopa lub smartfona nie powinno się zostawiać bez opieki na tylnym siedzeniu samochodu. Za każdym razem, gdy użytkownik odchodzi od swojego komputera, powinien go zablokować. W przeciwnym razie należy włączyć funkcję automatycznego blokowania na każdym urządzeniu używanym do celów służbowych. Wrażliwe dokumenty drukowane również nie powinny być pozostawiane bez nadzoru, a gdy nie są używane, należy je bezpiecznie przechowywać.

9 ZABEZPIECZ KOPIE ZAPASOWE

Aby umożliwić odzyskanie kluczowych formacji, należy utrzymywać kopie zapasowe, ponieważ są one skutecznym sposobem odzyskiwania danych po sytuacjach awaryjnych, takich jak atak ransomware. Należy stosować następujące zasady tworzenia kopii zapasowych:

- tworzenie kopii zapasowych jest regularne i w miarę możliwości zautomatyzowane,
- kopia zapasowa jest przechowywana oddzielnie od środowiska produkcyjnego MŚP,
- kopie zapasowe są szyfrowane, zwłaszcza jeśli mają być przenoszone między lokalizacjami,
- testuje się zdolność do regularnego przywracania danych z kopii zapasowych. Najlepiej byłoby przeprowadzać regularne testy pełnego przywrócenia systemu od początku do końca.

10 KORZYSTAJ Z CHMURY

Rozwiązania oparte na chmurze, choć oferują wiele korzyści, wiążą się z pewnym unikalnym ryzykiem, które MŚP powinny rozważyć przed nawiązaniem współpracy z dostawcą usług w chmurze. ENISA opublikowała „Cloud Security Guide for SMEs" („Przewodnik bezpieczeństwa w chmurze dla MŚP")[2], z którym MŚP powinny się zapoznać podczas migracji do chmury.

Wybierając dostawcę usług w chmurze, MŚP powinny upewnić się, że nie narusza ono żadnych przepisów lub regulacji poprzez przechowywanie danych, zwłaszcza danych osobowych, poza UE/EOG. Na przykład unijne RODO wymaga, aby dane osobowe osób zamieszkałych w UE/EOG nie były przechowywane ani przekazywane poza UE/EOG, chyba że na bardzo szczególnych warunkach.

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

11 ZABEZPIECZ STRONY INTERNETOWE

Istotne jest zapewnienie przez MŚP, aby ich strony internetowe były skonfigurowane i utrzymywane w bezpieczny sposób oraz aby wszelkie dane osobowe lub szczegóły finansowe, takie jak dane kart kredytowych, były odpowiednio chronione. Wiąże się to z przeprowadzaniem regularnych testów bezpieczeństwa stron internetowych w celu zidentyfikowania wszelkich potencjalnych słabości bezpieczeństwa i prowadzenia regularnych przeglądów w celu zapewnienia, że strona jest utrzymywana i aktualizowana prawidłowo.

12 POSZUKUJ INFORMACJI I DZIEL SIĘ NIMI

Skutecznym narzędziem w walce z cyberprzestępczością jest wymiana informacji. Wymiana informacji związanych z cyberprzestępczością ma kluczowe znaczenie dla MŚP, ponieważ pozwala im lepiej zrozumieć zagrożenia, na jakie są narażone. Firmy, które zasięgną informacji od podobnych sobie przedsiębiorstw o wyzwaniach związanych z cyberbezpieczeństwem oraz o tym, jak udało się je pokonać, z większym prawdopodobieństwem podejmą kroki w celu zabezpieczenia swoich systemów, niż gdyby miały usłyszeć podobne szczegóły z raportów branżowych lub ankiet dotyczących cyberbezpieczeństwa.

AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA

Informacje o ENISA
Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. ENISA – utworzona w 2004 r. i wzmocniona unijnym aktem o cyberbezpieczeństwie – wnosi wkład w politykę cybernetyczną UE, zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa, współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i zwiększanie świadomości, Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz, w efekcie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Aby uzyskać więcej informacji, zob.: 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