Cyberbezpieczeństwo

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369, z późn.zm.), zachęcamy Państwa do zapoznania się z informacjami, które przybliżą i pozwolą zrozumieć zagrożenia związane z cyberbezpieczeństwem, a także będą zawierały wskazówki w zakresie stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Bezpieczne hasła – jedna z najważniejszych zasad cyberhigieny

Większość usług internetowych, z których korzystamy wymaga od nas założenia konta, a następnie logowania się do niego za pomocą ustawionego przez nas loginu i hasła. To właśnie hasło jest swego rodzaju szyfrem do naszych danych, dlatego niezwykle ważne jest, aby było one silne i trudne do złamania. Jak zatem stworzyć takie hasło? Przede wszystkim powinno być trudne do odgadnięcia dla osób trzecich, ale łatwe do zapamiętania dla nas i składać się z co najmniej 12 znaków. Powinno być unikalne – jedno hasło do jednej usługi. Zgodnie z zaleceniami ekspertów CERT Polska hasła można budować za pomocą pełnych zdań zawierających co najmniej pięć wyrazów.

Niestety, nawet silne hasło nie zawsze może nas ochronić przed utratą konta lub wyciekiem danych. Żeby zwiększyć nasze bezpieczeństwo warto stosować dodatkową weryfikację podczas logowania. Wieloskładnikowe uwierzytelnianie (z ang. MFA - Multi-Factor Authentication) zapewnia ochronę podczas logowania się, poprzez dodatkową weryfikację tożsamości, np. skanowanie odcisku palca lub wprowadzenie kodu wysłanego do użytkownika na telefon, skrzynkę email. Obecnie najczęściej zastosowanie mają dwuskładnikowe etapy weryfikacji (z ang. 2FA two-factor authentication), z którymi można się spotkać podczas uzyskiwania dostępu do bankowości, poczty email czy kont w portalach społecznościowych.

Weryfikacja dwuetapowa - jak to działa?

Podczas konfigurowania 2FA użytkownik jest proszony o podanie „drugiego składnika weryfikującego", do którego dostęp ma tylko on. Zazwyczaj są to kody wysyłane na telefon (eksperci zajmujący się cyberbezpieczeństwem uznali, że nie jest już to najbezpieczniejsza metoda) lub jednorazowy kod/hasło wygenerowany przez aplikację zainstalowaną na urządzeniu moblinym (np. Microsoft Authenticator, Google Authenticator). Istnieją różne metody weryfikacji dwuetapowej, a jednym z najskuteczniejszych narzędzi, która może nas chronić przed utratą danych lub tożsamości są klucze U2F. Są to niewielkie urządzenia,

które przy pomocy USB możesz podłączyć do smartfona. Dzięki zastosowaniu w kluczach zaawansowanych metod kryptografii asymetrycznej powoduje, że przesyłane informacje nie trafią w ręce oszustów. Klucze U2F chronią nas nawet wtedy, gdy na fałszywej stronie internetowej podamy swoje dane. Na rynku dostępnych jest kilka rodzajów kluczy, warto przed zakupem porozmawiać ze sprzedawcą, który doradzi nam wybór. Więcej na temat uwierzytelniania dwuskładnikowego jest dostępne Łącze - kompleksowo o hasłach.

Programy antywirusowe – niezbędnik w trosce o naszą cyberhigienę

Jednym z najczęściej stosowanych sposobów, które chronią nasz sprzęt przed zainfekowaniem złośliwym oprogramowaniem są programy antywirusowe. Ważne, aby korzystać z nich w czasie rzeczywistym, używać ich do skanowania dysku, a przede wszystkim pamiętać o ich aktualizowaniu. Dzięki temu nasz antywirus będzie mógł na bieżąco odpowiadać na różne zagrożenia, zwłaszcza te najnowsze. Aby zwiększyć swoje bezpieczeństwo, zachęcamy również do korzystania z zapory sieciowej.

Aktualizuj swoje urządzenia, programy i aplikacje, z których korzystasz

Niestety nie zawsze urządzenia, oprogramowanie lub aplikacje, z których korzystamy są w pełni bezpieczne. Zdarza się, że znajdują się w nich błędy i luki bezpieczeństwa, które bardzo często są wykorzystywane przez cyberprzestępców. Regularna aktualizacja systemu operacyjnego, programów, aplikacji i przeglądarek internetowych z jakich korzystamy może uchronić nas przed atakiem cyberprzestępców. Aktualizacje zawierają poprawki, które chronią przed podatnościami i błędami. Jeśli nie będziemy ich stosować, nasze urządzenia mogą zostać zainfekowane.

Pomyśl zanim klikniesz, czyli zasada ograniczonego zaufania

Jedną z fundamentalnych zasad, o których powinniśmy pamiętać korzystając z internetu, to zasada ograniczonego zaufania. Rozwiązania technologiczne nie wystarczą, aby ustrzec się przed różnymi atakami cyberprzestępców. Musimy pamiętać, że oni stale szukają nowych sposobów i technik, by nas oszukać. Próbują nas zmanipulować, nakłonić do podjęcia działań, które mogą prowadzić do utraty naszych danych lub pieniędzy. Wykorzystują nasze emocje, naiwność oraz brak czasu i życie w biegu. Dlatego jeśli otrzymasz wiadomość, która nakłania Cię do podjęcia natychmiastowych działań, zastanów się czy jest ona prawdziwa. Uważaj również na różnego rodzaju wyjątkowe oferty, wygrane w loterii czy możliwość zainwestowania w kryptowaluty i inne sposoby na szybkie wzbogacenie się. Nie wchodź na strony, które wydają Ci się podejrzane i masz wątpliwości, czy są bezpieczne.

Dbaj o swoją prywatność w sieci

O tym, że anonimowość w sieci nie istnieje, wie już większość z nas. Każda nasza aktywność w internecie, zostawia po nas ślad cyfrowy. Istnieją jednak różne sposoby, by móc zwiększyć swoją prywatność w sieci. Jak to zrobić? Przede wszystkim pomyśl, zanim udostępnisz swoje zdjęcia, filmy lub inne informacje o sobie. Jeśli korzystasz z mediów społecznościowych, ogranicz widoczność swojego konta, sprawdź ustawienia prywatności. Zapoznaj się z regulaminem danego portalu i zastanów się, zanim zaczniesz udostępniać tam materiały. Korzystając z różnych komunikatorów internetowych, staraj się wybierać te, które są szyfrowane. Unikaj połączeń z publicznymi sieciami, a jeśli to konieczne, korzystaj z vpn'a. Pamiętaj, że tryb incognito nie chroni Cię przed wszystkim, nie pokazuje tylko twojej lokalizacji ani nie zapisuje historii. Jeśli chcesz zwiększyć swoją anonimowość, korzystaj z dedykowanych do tego przeglądarek.

Źródło: Łącze - jak chronić się przed atakami cyberprzestępców 30.12.2022 r.

Więcej informacji na temat cyberbezpieczeństwa znajdziecie Państwo na poniższych stronach:

- Łącze do bazy wiedzy o cyberbezpieczeństwie
- Łącze do Publikacji CERT Polska
- Łącze do CSIRT GOV
- Łącze do CSIRT NASK

Metadane

Data publikacji : 07.04.2023
Data modyfikacji : 30.11.2023
Rejestr zmian

Podmiot udostępniający informację:
Gdańskie Centrum Usług Wspólnych

Osoba wytwarzająca/odpowiadająca za informację:

Osoba udostępniająca informację:
Administrator

Osoba modyfikująca informację:
Administrator BIP
