Krajowy system cyberbezpieczeństwa

Wraz z wejściem w życie ustawy o krajowym systemie bezpieczeństwa na NASK (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy) został nałożony obowiązek koordynowania prac związanych z bezpieczeństwem cybernetycznym naszego kraju. Służby NASK przyjmują, analizują i podejmują działania na incydenty dotyczące bezpieczeństwa cywilnej cyberprzestrzeni RP zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny i osoby prywatne oraz na incydenty związane z nielegalnymi treściami publikowanymi w Internecie i zagrażającymi bezpieczeństwu dzieci oraz odpowiada za monitorowanie zagrożeń internetowych i stanu cyberbezpieczeństwa na poziomie sektorowym i krajowym (przejdź do ZGŁOSZENIA). **Podczas komunikacji elektronicznej z naszym urzędem, jednostkami podległymi lub innymi instytucjami zawsze zwracaj uwagę na bezpieczeństwo swoich danych i ochronę swoich urządzeń. Zalecaną formą kontaktu elektronicznego jest www.epuap.gov.pl oraz www.edoreczenia.gov.pl**

Cyberbezpieczeństwo – czy mnie to dotyczy?

Cyberbezpieczeństwo jest ważne, ponieważ smartfony, komputery i Internet są obecnie tak fundamentalną częścią współczesnego życia, że trudno sobie wyobrazić, jak moglibyśmy bez nich funkcjonować. Dlatego też szczególnie dziś ważne jest, aby w ramach kilku kroków ograniczyć cyberprzestępcom zdobycie dostępu do zawartości naszych urządzeń – smartfonów i komputerów – za ich pośrednictwem do naszych kont bankowych, kont w portalach społecznościowych, skrzynek poczty elektronicznej – zarówno prywatnych jak i służbowych.

Jak bronić się przed najpopularniejszymi atakami w cyberprzestrzeni i co to jest phishing oraz ransomware?

Phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Cyberprzestępcy podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet naszych znajomych, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont
społecznościowych, czy systemów biznesowych.
Nazwa phishing budzi dźwiękowe skojarzenia z fishingiem – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę". **Do tego wykorzystują najczęściej sfałszowane e-maile i SMS-y. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych (np. poprzez „metodę na BLIKa").**
Wiadomości phishingowe są tak przygotowywane przez cyberprzestępców aby wyglądały na autentyczne, ale w rzeczywistości są fałszywe. Mogą próbować skłonić Cię do ujawnienia poufnych informacji, zawierać linki do stron internetowych zainfekowanych szkodliwym oprogramowaniem, fałszywych stron płatności elektronicznych lub zawierać załącznik wyglądający jak interesujący dokument, który jednak w swojej treści zawiera złośliwy kod w celu przejęcia kontroli nad Twoim urządzeniem.

Jak radzić sobie z fałszywymi wiadomościami?

Jeśli nie kliknąłeś w żaden link w wiadomości e-mail, to dobrze.
Dopóki nie masz pewności, że nadawca jest prawdziwy, nie powinieneś klikać w żadne linki ani na nie odpowiadać. W wiadomościach SMS lub mailach często wykorzystywane są tzw. tiny-URL, czyli skrócone adresy stron internetowych. Stąd też zalecamy zwracanie szczególnej uwagi na nazwy stron internetowych, które przesyłane są w podejrzanych mailach czy SMSach np. zamiast www.allegro.pl wykorzystywany może być fałszywy adres www.allegrosklep.online itp. Następną rzeczą jest ustalenie, czy wiadomość e-mail jest autentyczna i nie jest oszustwem.
Jak rozpoznać e-mail wyłudzający informacje?

- Wiele wiadomości phishingowych ma niepoprawną gramatykę, interpunkcję, pisownię, czy też bak jest polskich znaków diakrytycznych np. nie używa się „ą", „ę" itd.
- Sprawdź, czy mail pochodzi z organizacji, na którą powołuje się nadawca. Często adres mailowy nadawcy jest zupełnie niewiarygodny, czy też nie jest tożsamy np. z podpisem pod treścią maila.
- Oceń, czy wygląd i ogólna jakość e-maila może pochodzić z organizacji / firmy, od której powinna pochodzić taka wiadomość np. użyte logotypy, stopki z danymi nadawcy itd.
- Sprawdź, czy e-mail jest adresowany do Ciebie z imienia i nazwiska, czy odnosi się do „cenionego klienta", „przyjaciela" lub „współpracownika"? Może to oznaczać, że nadawca tak naprawdę cię nie zna i że jest to część oszustwa typu phishing.
- Sprawdź, czy e-mail zawiera ukryte zagrożenie, które wymaga natychmiastowego działania? Bądź podejrzliwy w stosunku do słów typu „wyślij te dane w ciągu 24 godzin" lub „padłeś ofiarą przestępstwa, kliknij tutaj natychmiast".
- Spójrz na nazwę nadawcy, czy wygląda na prawdziwą, czy może tylko naśladuje kogoś, kogo znasz.
- Jeśli wiadomość brzmi zbyt dobrze, aby mogła być prawdziwa, prawdopodobnie nie jest ona prawdziwa. Jest mało prawdopodobne, aby ktoś chciał Ci dać pieniądze lub dostęp do tajnej części Internetu.
- Twój bank lub jakakolwiek inna instytucja nigdy nie powinna prosić Cię o podanie w wiadomości e-mail danych osobowych.
- Urzędy administracji publicznej nigdy nie proszą Cię przy pomocy SMS, czy maili o dopłatę do szczepionki, czy uregulowanie należności podatkowych.
- Sprawdź wszelkie polecenia lub pytania w wiadomości e-mail na przykład dzwoniąc do banku z pytaniem czy rzeczywiście wysłana została do Ciebie taka wiadomość lub wyszukaj w wyszukiwarce Google (lub podobnej) wybrane słowa użyte w wiadomości e-mail.
- Zwracaj uwagę na linki przekazywane również między znajomymi, sprawdź czy link faktycznie prowadzi do właściwej strony. Coraz częściej przestępcy uzyskując w nielegalny sposób kontrolę nad naszymi kontami społecznościowymi podszywając się pod naszych znajomych i rodzinę.
- Uważaj na skrócone linki, jeśli nie masz pewności dokąd poprowadzi Cię link, najedź wskaźnikiem myszy na link (nie klikaj), a na dole przeglądarki zostanie wyświetlony pełen adres linku.

Więcej informacji na temat cyberbezpieczeństwa i przykłady wyłudzania danych znajdziesz w załącznikach poniżej oraz na stronie NASK. Poniżej znajdują się biuletyny bezpieczeństwa wydawane cyklicznie w ramach programu "Partnerstwo dla Cyberbezpieczeństwa" (będą dodawane na naszą stronę systematycznie).