Cyberbezpieczeństwo

Cyberbezpieczeństwo
Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa publikujemy informacje na temat zagrożeń występujących w cyberprzestrzeni oraz porady jak zabezpieczyć się przed tymi zagrożeniami.
Cyberbezpieczeństwo zgodnie z obowiązującymi przepisami to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” (art. 2 pkt 4, Dz.U.2020.1369 t.j. z późn. zm.)

Incydent
Incydent oznacza zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Najczęstsze incydenty
- Złośliwe oprogramowanie (czyli wirusy, trojany, rootkity, scareware, ransomware przesyłane w postaci załączników do e-maili lub pobierane po kliknięciu w odnośnik zawarty w wiadomości pochodzącej od przestępcy),
- Ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji poprzez podszywanie się pod godną zaufania osobę lub instytucję),
- Spam (czyli niezamawiane wiadomości elektroniczne zawierające m.in. reklamy różnych usług i produktów, które mogą zawierać odnośniki do szkodliwego oprogramowania),
- Kradzież tożsamości,
- Kradzież, modyfikacja lub niszczenie danych.

Rodzaje zagrożeń w cyberprzestrzeni:
- Malware - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.
- Phishing - atak za pośrednictwem poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
- Spear Phishing - bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
- Atak typu “Man in the Middle” (MitM) - atak ten wymaga, aby napastnik znalazł się

między dwiema stronami, które się komunikują i był w stanie przechwytywać wysyłane informacje.
- Trojan – (koń trojański) - oprogramowanie, które podszywa się pod przydatne lub ciekawe dla użytkownika aplikacje, implementując szkodliwe, ukryte przed użytkownikiem różne funkcje (oprogramowanie szantażujące – ransomware, szpiegujące – spyware etc.).
- Ransomware - atak polegający na zaszyfrowaniu danych w systemie docelowym i zażądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych.
- Atak DoS lub DDoS - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. DDoS atakuje z wielu miejsc równocześnie.
- Ataki IoT w Internecie rzeczy - atak polegający na przejmowaniu kontroli nad urządzeniami w sieci Internet: inteligentnymi domami, budynkami, sieciami energetycznymi, urządzeniami gospodarstwa domowego - przemysłu etc.).
- Data Breaches (naruszenie danych) - atak tego typu polega na kradzieży danych. Motywy naruszeń danych obejmują przestępstwa: (tj. kradzieży tożsamości, chęci zawstydzenia instytucji, szpiegostwo i inne).
- Malware w aplikacjach telefonów. Urządzenia mobilne są szczególnie podatne na ataki złośliwego oprogramowania.

Podstawy ochrony przed zagrożeniami
- Nie zaniedbuj aktualizacji systemu operacyjnego i programów na używanym komputerze (najlepiej zaplanuj aktualizacje automatyczne).
- Posiadaj aktualny i wielofunkcyjny program antywirusowy z zaporą sieciową (ang. firewall). Stosuj ochronę w czasie rzeczywistym.
- Nie używaj prywatnych kont poczty elektronicznej i komunikatorów do korespondencji służbowej.
- Nie używaj prywatnych komputerów i telefonów do spraw służbowych.
- Nie używaj służbowych komputerów i telefonów do spraw prywatnych (w szczególności do czytania prywatnej poczty elektronicznej), nie udostępniaj ich członkom rodziny.
- Logując się na konto zawsze sprawdź czy domena danego portalu jest prawidłowa. Domena to nazwa zawierająca się między https://, a pierwszym kolejnym znakiem /
- Ignoruj wszystkie inne prośby o podanie swojego hasła, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi dezaktywacją konta.
- Pamiętaj, że żaden bank czy urząd nie wysyła e-maili do swoich

klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- Jeśli masz wątpliwości co do tożsamości osoby/instytucji za którą ktoś się podaje, zweryfikuj ją za pomocą innego środka komunikacji np. telefonicznie.
- Wszystkie podejrzane wiadomości na skrzynce służbowej zgłaszaj administratorom w swojej organizacji.
- O wszystkie podejrzane wiadomości na prywatnej skrzynce możesz zapytać CERT Polska (https://incydent.cert.pl / cert@cert.pl)
- Szczególnie podejrzane są wiadomości: zawierające załączniki, a zwłaszcza archiwa i dokumenty Office z hasłem podanym w treści wiadomości iwiadomości zmuszające do podjęcia natychmiastowej reakcji.
- Zachowaj ostrożność podczas otwierania załączników plików. Na przykład, jeśli otrzymasz wiadomość e-mail z załącznikiem PDF z opisem „zaległa faktura”, nie otwieraj go jeśli zobaczysz, że pochodzi on z nietypowego e-maila, takiego jak ann23452642@gmail.com ! Otwórz dopiero jeżeli masz 100% pewności, że wiesz kto wysłał wiadomość.
- Nie klikaj w odnośniki od nieznanych podmiotów, co do których nie masz pewności gdzie Cię zaprowadzą.
- Nie otwieraj plików, stron nieznanego pochodzenia.
- Stosuj długie hasła (powyżej 14 znaków).
- Dobrą metodą na długie hasło jest wymyślenie całej frazy, składającej się z kilku słów, np. 2CzerwoneRoweryJedzaNalesniki
- Unikaj haseł, które łatwo powiązać z publicznymi informacjami na temat Twojej osoby np. zawierających nazwisko, datę urodzenia itp.
- Hasło zmieniamy wtedy, gdy mamy podejrzenie, że mogła poznać je inna osoba. Nie ma potrzeby cyklicznej zmiany hasła.
- Nie używaj takich samych haseł na różnych serwisach, w szczególności do konta email, banku i innych wrażliwych kont, (więcej o tworzeniu haseł).
- Dla ułatwienia korzystaj z menedżerów haseł. Te wbudowane w przeglądarkę czy telefon są bezpieczne i proste w użyciu
- Włącz uwierzytelnianie dwuskładnikowe (tzw. 2FA) tam gdzie jest to możliwe. Uwierzytelnianie dwuskładnikowe w poczcie elektronicznej i w kontach społecznościowych jest konieczne. Jeżeli obecny dostawca Twojej poczty nie udostępnia uwierzytelniania dwuskładnikowego, zmień go. Najlepszym drugim składnikiem uwierzytelniania i jedynym odpornym na ataki phishingowe jest token sprzętowy U2F (np. YubiKey) (więcej o uwierzytelnianiu dwuskładnikowym).
- Zweryfikuj wszystkie dane kontaktowe w ustawieniach profilu poczty elektronicznej i mediów społecznościowych; dobra alternatywna metoda kontaktu ułatwi

odzyskanie utraconego konta.
- Jeżeli podejrzewasz, że ktoś mógł włamać się na twoje konto, zmień hasło, sprawdź dostępną w profilu historię logowania i zakończ wszystkie aktywne sesje.
- VPN nie chroni przed atakami phishingowymi i złośliwym oprogramowaniem!
- Do wrażliwej prywatnej komunikacji używaj komunikatorów szyfrowanych end-to-end, np. Signala.
- Używaj opcji automatycznego kasowania wiadomości po upływie określonego czasu – nie da się ukraść czegoś, czego już nie ma.
- Wykonuj kopie zapasowe ważnych danych.
- Weryfikuj adresy stron pod kątem literówek, łudząco podobnych lub powtarzających się znaków i porównuj je z oficjalnymi stronami (w szczególności w zakresie bankowości elektronicznej).
- Korzystaj wyłącznie ze stron i portali używających komunikacji szyfrowanej. Należy zweryfikować certyfikat SSL klikając w kłódkę przy adresie strony oraz zwrócić uwagę czy pierwszy człon adresu strony zaczyna się od https://
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.

Warto również zapoznać się z informacjami poniżej:
- Zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: https://www.cert.pl/ouch/
- Publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl/
- Poradniki na witrynie internetowej Serwis Rzeczypospolitej Polskiej https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo