Cyberbezpieczeństwo

Cyberbezpieczeństwo jest jednym ze strategicznych celów w obszarze bezpieczeństwa państwa i zapewnia ochronę instytucjom publicznym i niepublicznym-kluczowym w sektorze gospodarki, obywatelom i społeczeństwu. Jest to obszar wymagający stałego rozwoju i rozbudowy oraz śledzenia i umiejętności identyfikacji współczesnych jego zagrożeń.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

1. **Malware** - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.
2. **Phishing** - atak za pośrednictwem poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
3. **Spear Phishing** - bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
4. **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.
5. **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.).
6. **Ransomware** - atak polegający na zaszyfrowaniu danych w systemie docelowym i zażądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych.
7. **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.
8. **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.).
9. **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).
10. **Malware** w aplikacjach telefonów. Urządzenia mobilne są szczególnie podatne na ataki złośliwego oprogramowania.

Jak bezpiecznie korzystać z Internetu i nie stać się ofiarą cyberprzestępcy:

1. korzystać z e-usług lub portali internetowych tworząc długie i skomplikowane hasła dostępu ? co najmniej ośmioznakowe zawierające małe, wielkie litery, znaki specjalne lub cyfry. Dobrym rozwiązaniem jest korzystanie z tzw. haseł frazowych poprzez np zestawienie pięciu wyrazów niepowiązanych ze sobą i nieoddzielonych spacją,
2. dokonywać cyklicznych zmian haseł (średnio co 60 dni) oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej,
3. pliki zawierające Twoje dane osobowe przesyłać innym użytkownikom sieci za pośrednictwem poczty e- mail w formie zabezpieczonej hasłem, natomiast samo hasło przekazywać innym środkiem przekazu np. wiadomością sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata,
4. logując się na nieznane strony internetowe zwracać uwagę na poziom bezpieczeństwa danej strony ? symbolami znaczącymi o bezpieczeństwie są m.in. ?zielona kłódka? informująca, że strona jest wyposażona w sprawdzony i ważny certyfikat lub element ?https?, oznaczający, że strona jest szyfrowana. Dla pewności należy ?kliknąć? na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel,
5. w przypadku spostrzeżenia w adresie strony internetowej czerwonej kłódki ze znakiem krzyżyka, zachować szczególną ostrożność i powstrzymać się od wprowadzania danych, gdyż istnieje możliwość, iż ktoś podszywa się pod daną witrynę, aby przechwycić cenne informacje,
6. unikać umieszczania w tzw. publicznej chmurze plików i informacji zawierających wrażliwe dane na Twój temat;
7. unikać logowania się na swoje konta internetowe przy pomocy publicznego wifi lub na publicznych komputerach,
8. uważać na strony internetowe, które wymagają instalacji oprogramowania - w takim przypadku najlepiej uprzednio przeskanować wszystkie programy pobierane z internetu za pomocą aktualnego oprogramowania antywirusowego,
9. unikać otwierania nieznanych linków i załączników w wiadomościach e-mail;
10. unikać korzystania ze stron internetowych, w szczególności o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla użytkownika) oraz zwracać uwagę na reklamy wyświetlane na innych stronach internetowych które są przeglądane,
11. zwracać uwagę i upewnić się czy osoba, z którą nawiązywany jest kontakt jest tym, za kogo się podaje;
12. zwracać uwagę na wiadomości z prośbą o podanie szczegółów konta, gdyż instytucje finansowe oraz urzędy unikają takich sytuacji ze względów bezpieczeństwa;
13. zainstalować oprogramowanie antywirusowe i na bieżąco je aktualizować;

14. korzystać z najnowszych i zaktualizowanych wersji przeglądarek internetowych;
15. zapewnić, by system operacyjny posiadał włączoną funkcję automatycznych aktualizacji i instalować wszelkie aktualizacje zaraz po ich udostępnieniu przez producenta.

Serwisy społecznościowe

Serwisy społecznościowe są jednymi z najpopularniejszych stron odwiedzanych przez użytkowników internetu, służą przede wszystkim do utrzymywania kontaktów prywatnych i zawodowych oraz dzieleniem się opiniami i materiałami multimedialnymi. Korzystając z serwisów społecznościowych należy zachować ostrożność, ponieważ nieostrożne korzystanie z mediów społecznościowych może prowadzić m.in. do wycieku lub kradzieży wrażliwych danych, kradzieży tożsamości, kontaktu z niepożądanymi informacjami.

Korzystając z mediów społecznościowych pamiętaj:

1. zakładając profil należy rozważyć czy konieczne jest, aby profil zawierał imię i nazwisko użytkownika. Informacje publikowane w serwisach mogą dotyczyć również osób, które nie są jego użytkownikami. Dlatego warto monitorować informacje publikowane w internecie na swój temat w internecie i w razie konieczności podejmować stosowne kroki np. zgłosić krzywdzące/nieprawdziwe informacje do moderacji,
2. hasło umożliwiające logowanie do serwisu powinno być silne (składające się z losowych znaków) i inne niż wykorzystywane w pozostałych serwisach; w celu zwiększenia bezpieczeństwa zaleca się wprowadzenie podwójnej weryfikacji (za pomocą hasła sms). Zmiana hasła powinna nastąpić za każdym razem, jeśli występuje podejrzenie, że mogło zostać przechwycone lub po upływie 180 dni,
3. zakładając konto należy odpowiednio skonfigurować ustawienia prywatności zwracając szczególną uwagę na umożliwienie wyszukania profilu przez zewnętrzne wyszukiwarki, ustawienia odbiorców postów, możliwość oznaczania na zdjęciach i filmach, dostęp do znajomych czy lokalizacji, itp. Należy weryfikować regulamin oraz funkcjonalność serwisu, ponieważ wprowadzane zmiany mogą być kluczowe dla bezpieczeństwa,
4. zapraszanie znajomych lub przystępowanie do grup społecznościowych może prowadzić do ujawnienia prywatnych danych. Należy zwrócić uwagę również na to, do czego mają dostęp aplikacje oraz jakiego rodzaju dane są udostępniane w grach i quizach,
5. nie należy klikać w podejrzane linki oraz aplikacje; urządzenie z którego korzystamy powinno być na bieżąco aktualizowane. Jeśli zdarzy się, że musimy skorzystać z serwisu społecznościowego poza zaufanym urządzeniem lub siecią, należy pamiętać o wylogowaniu się z serwisu oraz zmianie hasła dostępu przy następnej wizycie,
6. pamiętaj, że informacją nie jest tylko tekst, ale również zdjęcie lub film (uwidoczniony adres na kopercie lub tabliczce, nr karty kredytowej, charakterystyczne obiekty pozwalające na identyfikację Twojego miejsca przebywania lub Twoich bliskich); polubione miejsca (jak również ?meldowania?) lub grupy do których należysz,
7. pamiętaj, że korzystając z serwisów społecznościowych łatwo można (również nieintencjonalnie) zdradzić poufne i wrażliwe dane osób trzecich, pracodawcy, kontrahenta. Publikując informacje lub zdjęcie zapytaj o zgodę osoby zainteresowane,
8. o ile nie pozwalają na to regulaminy pracodawcy, nie należy korzystać z prywatnych profili w celach zawodowych oraz przechowywać lub przesyłać dokumentacji służbowej za pomocą zewnętrznych nieautoryzowanych serwisów,
9. skasuj swój profil w serwisie, z którego nie będziesz więcej korzystać,
10. jeśli padłeś ofiarą przestępstwa internetowego nie kasuj żadnych danych, sporządź kopię całej korespondencji. Rozważ czasową zmianę ustawień prywatności na bardziej rygorystyczne,
11. reaguj na niebezpieczne zachowania innych użytkowników oraz publikowane przez nich treści niedozwolone i zgłaszaj do moderacji serwisu, wyspecjalizowanych zespołów reagujących lub Policji,
12. jeśli osoby niepełnoletnie korzystają z serwisów społecznościowych opiekunowie powinni podejmować kroki zwiększające ich bezpieczeństwo takie jak: rozmowy uświadamiające, bezwzględne reagowanie w przypadkach zagrożeń, zwiększenie rygorystyczności w ustawieniach prywatności oraz monitorowanie zachowań dziecka.

Bezpieczeństwo dzieci w internecie

Bezpieczne zachowania:

1. przed udostępnieniem dziecku sprzętu (np. telefon, tablet) przygotuj go konfigurując program antywirusowy i filtry kontroli rodzicielskiej, automatyczne płatności, ograniczenia czasowe oraz ustal z dzieckiem obowiązujące zasady (ograniczenia czasowe, rodzaj aktywności). Wymagaj, aby dziecko zgłaszało sytuacje kiedy się przestraszy lub spotka je coś nieoczekiwanego,
2. im mniejsze dziecko tym częściej monitoruj jego zachowania w sieci. Z nastolatkami rozmawiaj zarówno o treściach jak i osobach, które mogą spotkać w sieci i uczulaj na niebezpieczeństwa. Staraj się poznać znajomych dziecka tak samo, jakby to byli znajomi przychodzący do Waszego domu,
3. zwróć uwagę na zdjęcia i statusy, które publikujesz sam, oraz które publikują dzieci. Udostępnianie nieznajomym informacji o wyjeździe lub zdjęć z zajęć dodatkowych pozwala na poznanie miejsc Waszego przebywania i może sprowokować niebezpieczne sytuacje (np. włamanie do mieszkania czy porwanie dziecka),

4. nie publikuj zdjęć dziecka, gdzie jest niekompletnie ubrane, ponieważ mogą być atrakcyjne dla osób o pedofilskich skłonnościach. Nie publikuj ośmieszających zdjęć dzieci, ponieważ pokazuje to brak szacunku dla drugiej osoby,
5. reaguj na szkodliwe materiały publikowane w internecie. Zgłaszaj do moderacji lub wyspecjalizowanych zespołów (m.in. moderatorzy, działy abuse, www.dyzurnet.pl).

W przypadku podejrzenia, że dziecko utrzymuje kontakt z niebezpiecznym nieznajomym:

1. nie kasuj żadnych dowodów, zabezpiecz wszystkie rozmowy i przesłane materiały (zwróć szczególną uwagę na pornografię, manifesty polityczne, informacje o niebezpiecznych substancjach, dietach). Zabezpiecz również materiały wyprodukowane przez dziecko,
2. nie podejmuj samodzielnie kontaktu z osobą niebezpieczną, ponieważ może to utrudnić działania policji,
3. skontaktuj się z policją, wydrukuj kopie najważniejszych wiadomości. Możesz również zwrócić się do wyspecjalizowanych zespołów (www.116111.pl, www.dyzurnet.pl) lub pedagoga/psychologa szkolnego,
4. pamiętaj, że dziecko może być pod wpływem osoby, którą uważa za swojego przyjaciela. Dlatego działaj rozważnie, wpieraj dziecko i go nie obwiniaj. Zwróć uwagę na wszystkie możliwe kanały komunikacji (np. nieznany aparat telefoniczny czy profil na portalu społecznościowym).

W przypadku gdy natrafisz na szkodliwe materiały publikowane w internecie:

1. reaguj zgłaszając niebezpieczne zachowania do moderatorów,
2. jeśli masz podejrzenie, że materiały są nielegalne np. pornografia z udziałem dzieci, nakłanianie do samookaleczeń, zgłoś informację na policję lub wyspecjalizowanego zespołu,
3. nie rozsyłaj dalej szkodliwych materiałów i nie odpowiadaj na zaczepki ze strony innych użytkowników.

Bezpieczeństwo urządzeń mobilnych. Wskazówki dla podróżujących

Smartfony, laptopy czy tablety ? towarzyszą nam dzisiaj praktycznie na każdym kroku. Kiedy jesteśmy w podróży, pomagają nam w utrzymywaniu kontaktu ze światem. Urządzenia mobilne mogą także stanowić bogate źródło informacji zarówno o nas, jak i naszych bliskich: lista kontaktów, zdjęcia, filmy, historia lokalizacji, dane medyczne i finansowe. Niezależnie od tego, czy planujemy podróż służbową, czy wyjazd na wakacje, dobrze jest zadbać o ich bezpieczeństwo.

Phishing - niebezpieczne wiadomości

Pierwsza reakcja:

jeżeli otrzymałeś wiadomość e-mail od nieznanego nadawcy, lub taką której się nie spodziewasz, lub gdy cokolwiek w treści tej wiadomości wzbudzi Twój niepokój, nie klikaj w linki ani przyciski graficzne w treści, ani w załączniki. Grozi to zarażeniem komputera złośliwym oprogramowaniem.

Ocena sytuacji:

złośliwa wiadomość może być powiadomieniem na temat czegoś co nas nie dotyczy, np. informacją o fakturze za towar czy usługę której nie zamawialiśmy, awizem dotyczącym przesyłki której nie oczekujemy.
Nadawcą takiej wiadomości są cyberprzestępcy którzy w ten sposób chcą zarazić Twój komputer złośliwym oprogramowaniem i tą drogą przejąć nad nim kontrolę, np. w celu wyłudzenia loginu i hasła do internetowego banku, skrzynki pocztowej, czy mediów społecznościowych.

Reakcja:

jeśli podejrzana wiadomość wygląda jak wysłana ze znanej Ci instytucji czy przez znaną Ci osobę, skontaktuj się telefonicznie z nadawcą i ostrzeż go, że w jego imieniu wysyłane są fałszywe wiadomości.
Wiadomość wyeksportuj wraz z załącznikami i nagłówkami do pliku w formacie EML i prześlij na adres cert@cert.pl albo zgłoś jako incydent w formularzu na stronie https://www.cert.pl/zglos-incydent/, załączając plik EML. Jeżeli nie potrafisz tego zrobić, poproś znajomego o pomoc, lub skontaktuj się z zespołem CERT Polska (cert@cert.pl) w celu uzyskania dodatkowych wskazówek.

Ransomware

Złośliwe oprogramowanie jest jednym z największych zagrożeń dla indywidualnego użytkownika komputera osobistego. Szczególnie groźne jest oprogramowanie szyfrujące dla okupu dane użytkownika (zwane także "ransomware"). Oprogramowanie to ma jeden cel ? zmusić użytkownika aby zapłacił okup za przywrócenie dostępu do swoich danych.

Większość rodzin złośliwego oprogramowania tego rodzaju używa mocnych, nowoczesnych szyfrów których nie da się łatwo złamać. Po zaszyfrowaniu danych na zarażonym komputerze, wirus wyświetla użytkownikowi groźnie wyglądający komunikat żądający pieniędzy za udostępnienie klucza albo programu odszyfrowującego. Niektóre odmiany ransomware blokują

całkowicie dostęp do systemu operacyjnego, czyniąc sprzęt zupełnie bezużytecznym.

Atakowane są także urządzenia z systemem Android. Ponieważ system ten zazwyczaj uniemożliwia aplikacji dostęp do danych innych programów, telefon jest blokowany przez nakłonienie użytkownika aby zezwolił złośliwemu programowi na korzystanie z funkcji zarządzania telefonem, po czym ustawiana jest blokada ekranu na długie, nieznane właścicielowi urządzenia hasło.

Niebezpieczeństwo dla sieci firmowych:

Atak ransomware jest szczególnie niebezpieczny dla infrastruktury firmowej - jeśli złośliwy program zostanie uruchomiony na komputerze mającym prawa zapisu do zasobów sieciowych na których przechowywane są firmowe dane, zostaną one zaszyfrowane razem z danymi znajdującymi się na bezpośrednio zaatakowanym komputerze.

Droga infekcji

Złośliwe oprogramowanie tego typu może być rozpowszechniane na różne sposoby:

1. rozsyłane jako złośliwe załączniki w wiadomościach e-mail zachęcających do kliknięcia
2. instalowane przez złośliwe strony WWW
3. instalowane przez złośliwe reklamy na legalnych stronach WWW
4. instalowane za pomocą złośliwego oprogramowania, którym komputer był już zarażony wcześniej
5. instalowane poprzez nieuprawniony zdalny dostęp do komputera

Obrona przed ransomware

Obronić się przed tym typem ataku jest bardzo trudno. Należy zachowywać ostrożność przeglądając strony internetowe, warto zainstalować w przeglądarce wtyczkę blokującą reklamy, podejrzliwie też należy się odnosić do sytuacji zachęcających nas do kliknięcia w nietypowy odnośnik albo uruchomienia nieznanego programu. Jednak właściwie jedynym pewnym sposobem na zabezpieczenie się jest tworzenie na bieżąco kopii zapasowych swoich danych. Jeżeli nasz system ma funkcję wykonywania na bieżąco kopii zapasowej danych, warto z niej skorzystać, jednak należy pamiętać że bardziej rozbudowane wersje ransomware usuwają część automatycznie zapisywanych kopii danych i systemu. Podobnie w wypadku firm i większych organizacji ważne jest podnoszenie świadomości użytkowników oraz wdrożenie odpowiednich procesów ochrony danych.

Indywidualni użytkownicy mogą sobie ułatwić tworzenie kopii zapasowych przez korzystanie z wirtualnych dysków w chmurze, niektóre takie serwisy nie tylko pozwalają z łatwością dzielić się plikami ale też zapisują historię zmian. Jeśli dane na takim dysku zostaną zaszyfrowane przez ransomware, użytkownik może je odzyskać sięgając do wcześniejszych wersji.

Należy też aktualizować system i zainstalowane aplikacje kiedy pojawiają się uaktualnienia oraz w przypadku komputerów stacjonarnych zainstalować i uruchomić program antywirusowy, już nawet dostępny za darmo dla wszystkich użytkowników Windows program Defender stanowi znaczącą ochronę.

Po ataku

Jeśli jednak staniemy się celem i nasze dane zostały zaszyfrowane, należy sprawdzić stronę https://www.nomoreransom.org/ na której znajdują się narzędzia do odzyskiwania plików zaszyfrowanych przez kilka rodzin ransomware - jeśli cyberprzestępcy popełnili błędy, istnieje szansa na odzyskanie danych. Warto też zgłosić atak do CERT Polska pod adresem https://cert.pl/ - specjaliści z CERT gromadzą informacje o atakach ransomware i tworzą narzędzia do odszyfrowywania danych i zwalczania tego typu ataków.

Cyber słownik

1. CERT/CSIRT - (Computer Emergency Response Team/Computer Security Incident Response Team) - określenie zespołu reagowania na incydenty komputerowe patrz: Zespół Reagowania na Incydenty Komputerowe
2. CERT Polska - pierwszy w Polsce zespół reagowania na incydenty komputerowe, powołany w strukturach NASK ? Naukowej i Akademickiej Sieci Komputerowej (www.cert.pl)
3. CSIRT GOV - rządowy zespół reagowania na incydenty komputerowe
4. CSIRT MON - zespół reagowania na incydenty komputerowe w resorcie obrony narodowej
5. DoS (denial of service; dosłownie: odmowa usługi) - atak, którego skutkiem jest uniemożliwienie dostępu do usługi na serwerze (na przykład skorzystania ze strony www)
6. DDoS (distributed denial of service) - atak DoS przeprowadzany z wielu źródeł jednocześnie
7. Dyżurnet.pl - działający w NASK - Naukowej i Akademickiej Sieci Komputerowej punkt kontaktowy do zgłaszania nielegalnych treści w Internecie szczególnie treści przedstawiających seksualne wykorzystywanie dzieci (www.dyzurnet.pl)
8. Incydent (incydent komputerowy) - zdarzenie zagrażające lub naruszające bezpieczeństwo sieci Internet

9. Luka - błąd w oprogramowaniu, który ma wpływ na bezpieczeństwo jego użytkowania
10. Poprawka bezpieczeństwa (patch, łata) - oprogramowanie, zwykle dostarczane przez producenta, usuwające lukę
11. Malware (od malicious software) - patrz: złośliwe oprogramowanie
12. Phishing - atak mający na celu wydobycie informacji (np. hasła) przez podszycie się pod zaufany podmiot (na przykład bank)
13. Ransomware (od ransom = okup i malware) - rodzaj złośliwego oprogramowania, które uniemożliwia użytkownikowi dostęp do jego danych (najczęściej przez zaszyfrowanie), a do przywrócenia go wymaga wpłacenia okupu
14. Szyfrowanie - proces przekształcania informacji w taki sposób, że jej odczytanie nie jest możliwe bez znajomości tzw. klucza odszyfrującego
15. Zespół Reagowania na Incydenty Komputerowe - zespół tworzony przez ekspertów, posiadających odpowiednią wiedzę i doświadczenie oraz procedury postępowania w przypadku wystąpienia incydentu; do głównych zadań Zespołu należy przyjmowanie zgłoszeń o incydentach bezpieczeństwa sieciowego oraz analiza bieżących zagrożeń występujących w sieci Internet
16. Złośliwe oprogramowanie - oprogramowanie, którego działanie powoduje szkody dla użytkownika

Odnośniki do stron dotyczących cyberbezpieczeństwa:

1. poradniki na witrynie internetowej Serwis Rzeczypospolitej Polskiej https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
2. publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl
3. 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
4. strona internetowa kampanii STÓJ. POMYŚL. POŁĄCZ mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: https://stojpomyslpolacz.pl/stp