Zagrożenia w sieci

Bezpieczne korzystanie z portali społecznościowych i zarządzanie tożsamością oraz własnym wizerunkiem w sieci.

Posiadanie profilu na popularnym portalu społecznościowym jest obecnie pożądane, a często wymagane. Użytkownicy sieci społecznościowej dzielą się swoimi prywatnymi informacjami i zdjęciami z innymi, nie zdając sobie sprawy z tego, że każdy ich wpis może zostać wykorzystany w niepożądany sposób. Bardzo łatwo określić preferencje użytkownika, stworzyć jego społecznościowe Curriculum Vitae, a następnie wykorzystać te informacje do zdobycia jego zaufania, uzyskania innych prywatnych informacji, dotarcia do danych, które atakujący chce przechwycić.

1. Typy zagrożeń dla informacji na portalach społecznościowych.

Korzystanie z portali społecznościowych, poza oczywistymi zaletami, niesie również wiele zagrożeń. Wszystkie informacje, które świadomie lub nieświadomie udostępniamy mogą stać się celem ataku. W przypadku portali społecznościowych należy pamiętać, że niezależnie od tego, jak bardzo użytkownik się zabezpieczy, jego bezpieczeństwo w znacznym stopniu zależy od jego własnych ustawień prywatności na portalu i ustawień prywatności jego znajomych.

Podstawowym zagrożeniem, z jakim musimy się liczyć, jest:

- Zbieranie danych o użytkownikach, cyfrowych dossier, czyli odpowiedników CV. Są to wszystkie informacje, które użytkownicy sami publikują: swoje miejsca zamieszkania, informacje o wykształceniu, wykonywanej pracy, swoje zdjęcia, kontakty, statusy, polubione strony lub linki. Wszystkie te informacje i dane osobowe mogą zostać użyte przeciw publikującym je osobom.
  ***PRZYKŁAD**: odzyskiwanie hasła do profilu użytkownika.*
- Można też zbierać dane historyczne, które już kiedyś użytkownicy opublikowali. Dane te mogą zostać użyte do różnych celów, często w sposób niekorzystny dla autorów publikacji.
- Do standardowych sposobów pozyskiwania danych o użytkownikach należy ***rozpoznawanie twarzy*** - wystarczy, że dana osoba została oznaczona na zdjęciu znajomych z portalu. Można również wyszukiwać obrazy po zawartości CBIR (ang. content-based image retrieval), podobnie jak w przypadku rozpoznawania twarzy. Na zdjęciach można oznaczać lokacje geograficzne, przedmioty i inne cechy.
- **Pozyskiwaniu danych** i informacji sprzyjają trudności z całkowitym usuwaniem kont na portalach społecznościowych. Wszystkie dane udostępniane tym portalom są przechowywane na serwerach zewnętrznych, dlatego nawet w przypadku usunięcia profilu, kopia tych danych nie jest usuwana.
- Do poważnych zagrożeń należy ***spam***. Jak w każdym popularnym medium informacyjnym, trzeba się liczyć z otrzymywaniem niechcianych wiadomości i reklam.
- Bardzo ważne zagrożenia to XSS (ang. cross site scripting), ***wirusy oraz robaki***.

- ***Agregatory*** SNS (ang. social networking service), powielające portale społecznościowe dla niewielkiego grona użytkowników. W rzeczywistości agregatory są sposobem na pozyskiwanie lub wyciąganie informacji.
- Ważnym zagrożeniem jest ***phishing***. Jest to stosowanie taktyk socjotechnicznych (ang. social engineering) do wydobywania od użytkowników ich sekretnych informacji.
- ***Przejmowanie profili i szarganie reputacji*** w wyniku kradzieży tożsamości.
- Szczególnie dokuczliwym zagrożeniem jest wykorzystywana niekiedy możliwość zwyczajnego ***znęcania się***, poprzez wysyłanie obraźliwych wiadomości, szantaż i nękanie użytkowników i osób.

Największą luką w zabezpieczeniach portali są sami użytkownicy. Zdecydowana większość zagrożeń jest propagowana przez nieświadomość członków społeczności. Bez ich udziału nikt nie byłby w stanie wykorzystać możliwości kradzieży ich danych. Portale wprowadzają coraz nowsze zabezpieczenia, lecz jak długo bezpieczeństwo użytkownika będzie zależało przede wszystkim od niego samego, tak długo on, jego reputacja i profil oraz jego sekretne dane, będą w ciągłym zagrożeniu.

Dziecko nieodpowiednie treści często znajduje przypadkowo. Czasami wystarczy kliknąć o „jeden raz za dużo". Przez co dzieci mają dostęp do: pornografii, przemocy – filmy i zdjęcia, materiałów nawołujących do nietolerancji, materiałów przedstawiających niebezpieczne postawy życiowe (hazard, anoreksja, używki, sekty, narkotyki, samouszkodzenia), nieadekwatnych usług handlowych. Odbiór treści niedostosowanych do wieku i rozwoju dziecka może powodować:

- zafałszowany obraz świata,
- zaburzony rozwój psychomotoryczny,
- zaburzenia emocjonalne,
- promocję złych wzorców,
- podejmowanie działań na szkodę swoją i innych.

2. Zawieranie znajomości w Internecie, zjawisko groomingu.

Internet stwarza dzieciom i młodzieży możliwości odkrywania, zawierania znajomości i tworzenia w sieci. Z jego używaniem wiążą się jednak także zagrożenia.

DYSKUSJA:

- *Jak rodzice mogą pomóc dzieciom w zminimalizowaniu tych zagrożeń?*
- *Gdzie szukać pomocy, jak rozpoznać zagrożenie?*

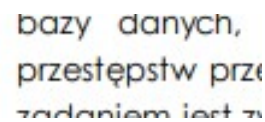
Dla dzieci i młodzieży Internet to miejsce spotkań, w którym mogą natknąć się osoby obce. W sieci można doświadczyć przykrości, napastowania, a nawet przemocy. Przede wszystkim trzeba poinformować dzieci o zagrożeniach istniejących w Internecie, żeby umiały zachowywać się bezpiecznie, oraz być gotowym do omówienia z nimi wszystkich wątpliwości, jakie mogą powstać w związku z korzystaniem z sieci. Należy przypominać im, aby nie podawały swoich danych osobowych, gdyż to jest główne źródło zagrożeń. Tożsamość użytkownika można odkryć poprzez powiązanie różnych informacji, jakie o sobie podaje, np. nazwy szkoły, klubu sportowego, regionu zamieszkania itp. Do nich zaliczają się różnego rodzaju artykuły, fora internetowe, zdjęcia lub filmy mające charakter przemocowy, pornograficzny oraz nawołujący do nietolerancji wobec ludzi innej rasy, narodowości lub wyznania.

Z pomocą przychodzi przygotowany przez Fundację Orange kurs „Bezpiecznie Tu i Tam". Skierowany do rodziców dzieci w różnym wieku, jest dostępny bezpłatnie pod adresem http://www.fundacja.orange.pl/kurs

ĆWICZENIE: Rozwiązywanie testu „Podstawy bezpieczeństwa w Internecie" *na stronie* http://www.fundacja.orange.pl/kurs

1. Rozwiązywanie testu
2. Zapoznanie się z ideą programu „Bezpiecznie Tu i Tam".

Bardzo niebezpiecznym zjawiskiem jest ***GROOMING*** – czyli uwodzenie dzieci w sieci. Uwodzący dziecku obiecuje przyjaźń i wsparcie. Pozyskuje filmy i zdjęcia, prosi o spotkanie. Jeżeli dziecko się nie zgadza grozi upublicznieniem intymnych materiałów (filmy, zdjęcia, zapisy rozmów internetowych). Zjawisko niezwykle niebezpieczne ze względu na daleko idące konsekwencje i zagrożenie poważną traumą.
Dzieci czasami padają ofiarą **cyberprzestępstw** lub same, często nieświadomie, są ich sprawcami. Należą do nich: włamania, nielegalne kopiowanie, nieuprawnione niszczenie danych, korzystanie z nielegalnego oprogramowania.
CSAM - to angielski zwrot, używany w Europie, przede wszystkim przez policję i inne instytucje, które zajmują się problematyką wykorzystywania dzieci. Osoby produkujące materiały CSAM nie są tylko wytwórcami nielegalnych treści. Dokonują też gwałtów, które następnie utrwalają na filmie lub fotografii. Za każdym materiałem pornograficznym z udziałem dziecka zawsze stoi wykorzystanie seksualne. W przypadku CSAM, dziecko przedstawione jest w seksualnym kontekście wbrew swojej woli i doznaje realnej krzywdy. Takie treści z udziałem dzieci są nielegalne, a za ich dystrybucję grozi więzienie. Termin **„pornografia dziecięca"** przyjął się w języku. Gdy natrafisz na CSAM w Internecie, powinieneś zgłosić ten fakt do Dyżurnet.pl. Zespół interwencyjny ds. nielegalnych treści w Internecie zadba o to, aby materiały te zostały usunięte. Przekaże też wszystkie informacje o nim do międzynarodowej bazy danych, która pomaga identyfikować ofiary, sprawców i miejsca popełnienia przestępstw przeciwko wolności seksualnej dzieci. Z bazy korzystają organy ścigania, których zadaniem jest zwalczanie tego typu przestępczości[1].



Statystyki policyjne ujawniają, 80% zdjęć o charakterze pornograficznym zostaje wytworzonych przez dzieci, one same są ich dostawcami. Utrwalają je za pośrednictwem kamer internetowych, czy aparatów cyfrowych pod wpływem manipulacji i gratyfikacji ze strony poznanych w Sieci osób dorosłych.

Opracowała: ELŻBIETA FIM

[1] *https://reagujzglos.dyzurnet.pl/download/czym_tak_naprawde_jest_pornografia.pdf*