sieć na kulturę

PROJEKTOWANIE I REALIZACJA SERWISÓW INTERNETOWYCH ORAZ GIER MOBILNYCH

PODRĘCZNIK

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
FWZR
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Wprowadzenie

Strony internetowe, portale społecznościowe, gry komputerowe, webowe i mobilne zagościły już na dobre w naszym życiu codziennym. Surfujemy po internecie, gramy na komputerach, konsolach, smartfonach, w domu, w poczekalni, autobusie, w sklepie, wspólnie, ze znajomymi i samodzielnie. Wielu młodych ludzi wiąże swoją przyszłość z branżą IT, szczególnie, że w Polsce dobrze się ona rozwija. Warto zatem poznać zasady i najważniejsze zagadnienia z obszaru projektowania i realizacji serwisów internetowych oraz gier mobilnych, nie tylko by aktywnie tworzyć i umieszczać własne treści, ale także by być świadomym i odpowiedzialnym użytkownikiem.

Niniejszy podręcznik zawiera informacje na temat tego jak wygląda proces tworzenia stron www lub aplikacji, czym jest i jaka jest różnica pomiędzy UI - interfejs użytkownika i UX - doświadczenie użytkownika, co to jest gra, na czym polega projektowanie gier, jakie są elementy, z których składa się gra, gatunki gier, a także co to jest i czemu służy grywalizacja.

Przedstawia również opracowanie na temat tego jak zabezpieczyć swoją stronę i aplikację przed włamaniem i kradzieżą danych użytkowników.

Jak projektować strony www lub aplikacje?

Proces tworzenia stron www i aplikacji można podzielić na trzy główne etapy:

1. etap przygotowania koncepcji, w którym projektujemy aplikację i testujemy jej prototyp, czyli pierwowzór z odbiorcami,
2. etap wytwarzania oprogramowania, w którym programujemy aplikację, wykonujemy potrzebne do niej grafiki, piszemy teksty, przeprowadzamy różne testy techniczne i funkcjonalne,
3. etap utrzymania, który następuje po publikacji, czyli udostępnieniu strony lub aplikacji, a w którym pilnujemy, by aplikacja dobrze działała i w razie czego ją poprawiamy.

Poniżej omówimy kroki i elementy związane z etapem przygotowania koncepcji strony www lub aplikacji, czyli projektowania. Projektowanie zaczynamy od zastanowienia się dla kogo jest strona lub aplikacja i na jakie potrzeby odbiorcy odpowiada: np. informuje o czymś ciekawym, pozwala coś wykonać, np. zrobić zakupy. Musimy przemyśleć jej funkcje, jakie powinny one być, aby strona lub aplikacja spełniała swoje zadanie.

Następnie wykonujemy jej szkic ołówkiem lub w formie prostego schematu. Szkic lub schemat pozwala szybko zorientować się z jakich elementów składa się strona, jakie są ich proporcje, które informacje są ważniejsze, czyli większe lub bardziej kontrastowe, a które są mniej ważne mniejsze. Dopiero potem dobieramy kolory i dodajemy zdjęcia i grafiki, czyli tworzymy wygląd strony lub aplikacji.

Więcej o projektowaniu i publikacji aplikacji i gier mobilnych można przeczytać w bezpłatnej publikacji pt. Appetyt na applikacje, S. Żółkiewska, wyd. Fundacja Orange 2016, dostępnej na stronie fundacji:

https://fundacja.orange.pl/files/user_files/user_upload/publikacje/APPetyt_na_APPlikacje_praktyczny_przewodnik_2016.pdf

UI I UX

Choć na pierwszy rzut oka na stronach i w aplikacjach widzimy zazwyczaj kolorowe zdjęcia i przyciski, to podczas projektowaniu strony warto pamiętać, że liczy się nie tylko wygląd interfejsu (czyli UI, ang. user interfejs), lecz także nawigacja i architektura informacji,

czyli całe doświadczenie użytkownika (inaczej UX lub po angielski user experience): to, w jaki sposób korzysta on ze strony, czy jest to dla niego intuicyjne, zrozumiałe.

Dobrym porównaniem, które może pomóc zrozumieć, czym różni się UX i UI jest przykład ciastka: Wyobraźmy sobie, że UI (interfejs użytkownika) to wygląd ciastka. Mówi się czasami, że 'jemy oczami', gdy jakieś danie jest ładnie podane i dobrze wygląda. Jednak czym innym jest smak ciastka i nasze wrażenia, gdy je jemy. Może się okazać, że ładnie wyglądające ciastko nie jest zbyt smaczne. Pamiętajmy jednak, że wygląd ciastka wpływa na to, czy zechcemy po nie sięgnąć i je zjeść, a w przypadku strony internetowej - czy przykuje ona naszą uwagę na tyle, że zechcemy z niej korzystać.

PROJEKTOWANIE UI

Dlatego też nim dowiemy się jak projektować doświadczenie użytkownika, warto dowiedzieć się na czym polega projektowanie interfejsu, ponieważ - jak już wiemy - dobry UX nie może istnieć bez dobrego UI i na odwrót. Projektowanie UI to świadomy dobór kolorów, kształtów, typografii i proporcji między nimi w taki sposób, aby jak najlepiej oddać funkcje programu, gry, lub aplikacji i uwzględnić upodobania użytkownika. Użytkownik oznacza tutaj odbiorcę, kogoś, kto używa naszej strony lub aplikacji, dla kogo jest ona przeznaczona.

Warto pamiętać, że każdy użytkownik ma nieco inne potrzeby i upodobania. Dlatego nim przystąpimy do projektowania, warto je lepiej poznać. Jak? Na kilka sposobów: można poszukać informacji o nim w internecie, dowiedzieć się, jakie np. kolory lubią osoby w starszym wieku i dlaczego. Można też zapytać o upodobania osoby z danej grupy wiekowej np. w formie ankiety lub wywiadu.

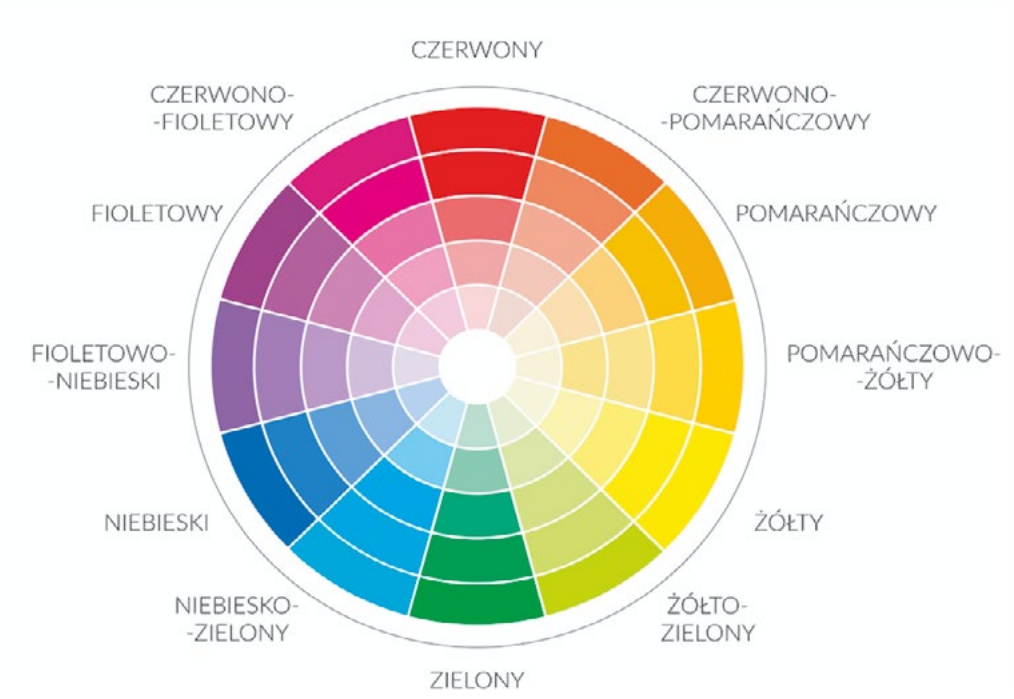
ELEMENTY UI (INTERFEJSU UŻYTKOWNIKA)

Najważniejsze elementy wizualne, graficzne, z których składa się interfejs to:

1. kolory
2. kształty (obły, ostry itd.)
3. krój pisma (inaczej typografia, lub też potocznie: czcionka)

Pomówmy najpierw o kolorze. Kolor to najmocniejszy, niewerbalny nośnik informacji. Przekaz, który trafia bezpośrednio do podświadomości. Oznacza to, że wywołuje on w nas emocje nawet gdy nie jesteśmy tego świadomi.

Każdy kolor ma swoją symbolikę. Wynika ona z naszej kultury, ale i z podstawowych skojarzeń elementów przestrzeni nas otaczających: błękitnego, spokojnego nieba czy trawy, słońca i ognia. Dlatego właśnie np. żółty kojarzy się nam z ciepłem, optymizmem (słońce jest żółte), a czerwony z energią czy pobudzeniem do działania (ogień jest czerwony). Znane firmy świadomie wykorzystują te skojarzenia w swoich projektach, aby tak właśnie postrzegali je ich odbiorcy.



Źródło obrazka: https://archistacja.pl/index.php/2017/01/19/jak-dobierac-kolory-we-wnetrzu/kolo-barw/

Powyżej widzimy koło barw, na którym widać, jak mieszają się ze sobą i przenikają poszczególne kolory. Kolory podstawowe, takie jak: niebieski, żółty i czerwony to kolory, z których - po ich zmieszaniu - można uzyskać kolory pochodne, czyli np. zielony (żółty+niebieski) lub pomarańczowy (czerwony+żółty). Każdy kolor ma też swój odcień i natężenie. Te jaśniejsze są odbierane jako bardziej delikatne, a mocniejsze - jako bardziej zdecydowane. Warto pamiętać, że kolory, które znajdują się naprzeciw siebie na kole barw, czyli np. zielony i czerwony lub niebieski i pomarańczowy, tworzą najbardziej kontrastowe pary. Mogą więc stanowić zbyt mocne zestawienie na stronie internetowej. Bezpieczniej jest zestawiać barwy znajdujące się niedaleko siebie, np. fioletowy i pomarańczowy.

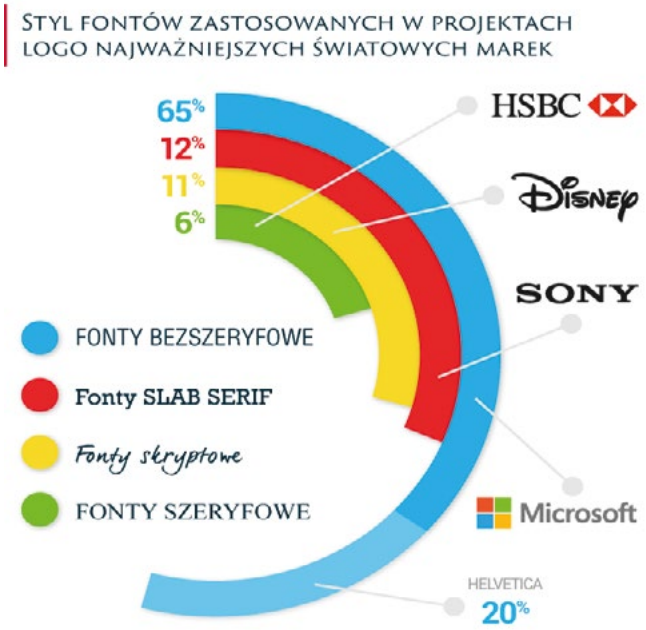
Więcej o kolorach i tym jak działają na innych można przeczytać na blogu projektowaniegraficzne.pl:

https://www.projektowaniegraficzne.pl/znaczenie-kolorow-w-reklamie-teoria-barw-psychologi-kolorow/

Kolejnym ważnym elementem, na którym możemy oprzeć swój projekt wyglądu strony internetowej jest dobór odpowiednich kształtów. Kształt silnie oddziałuje na podświadomość. Kształty ostro zakończone postrzegane są jako męskie, kształty obłe - jako żeńskie, dziecięce.

Kształty mogą być statyczne (kojarzą się wtedy z czymś miłym, bezpiecznym) lub dynamiczne (wówczas sugerują ruch, postęp). Wybór kształtów, z jakich będą składały się elementy na stronie wpływa na to, jak zostanie odebrana przez użytkownika. Jeśli np. przyciski na stronie będą prostokątami o zaokrąglonych rogach, to będą odbierane jako przyjemne, bezpieczne i delikatne. Jeśli będą np. dynamicznymi wielokątami, będą wprowadzały wrażenie ruchu i niepokoju. To od charakteru naszej strony i tego, jakie wrażenie chcemy, żeby sprawiała, zależy rodzaj kształtów, jakie powinniśmy zastosować.

Kolejnym ważnym elementem projektowania interfejsu jest typografia lub czcionka, font, a mówiąc poprawnie: krój pisma. Tak jak w przypadku kształtów: różne kroje pisma mogą przekazywać różne emocje i w różny sposób podkreślać wybrane elementy interfejsu. Na ekranach najlepiej sprawdzają się czcionki jednoelementowe, bezszeryfowe, zbudowane z linii o jednej grubości. Wtedy nawet gdy ekran mocno świeci, to jesteśmy w stanie zobaczyć cały kształt litery i dobrze ją odczytać.



Źródło obrazka:
https://snowball.com.pl/blog/kolory-czcionki-ktore-napedzaja-najlepsze-marki-swiecie/

Wykres powyżej przedstawia cztery główne rodzaje czcionek i to jak często są wykorzystywane w projektach znanych marek. Widać, że najpopularniejsze są proste czcionki jednoelementowe, bezszeryfowe, takie jak w logo firmy Microsoft.

UX (DOŚWIADCZENIE UŻYTKOWNIKA)

Jak wspomnieliśmy powyżej: UX i UI są ze sobą powiązane i połączone, dlatego dobre doświadczenie użytkownika nie istnieje bez dobrego projektu UI. Doświadczenie użytkownika to w skrócie wszystkie wrażenia, jakie ma użytkownik podczas korzystania z naszego produktu, usługi lub strony www. Obejmuje ono m.in.:

- ogólny wygląd interfejsu (kolory, kształty, proporcje, czcionka)
- użyteczność (jak szybko i sprawnie użytkownik może zrobić to, czego potrzebuje)
- zawartość (teksty, multimedia)

Źródło obrazka: https://dailyweb.pl/a-wiec-chcesz-byc-uxem-pozwol-ze-ci-pomoge/

Na ilustracji powyżej wierzchołek góry lodowej to UI - interfejs użytkownika, to co widzimy na pierwszy rzut oka. UX, czyli user experience to ta część góry lodowej, która znajduje się pod wodą. Jest niewidoczna na pierwszy rzut oka, ale stanowi jej dużą i bardzo ważną część.

Jak zaprojektować dobre doświadczenie użytkownika do strony lub aplikacji? Po pierwsze

postarać się zrozumieć i poznać użytkownika: co lubi, jakie ma problemy i bariery (np. czy ma słabszy wzrok). Po drugie warto znaleźć i przetestować jak najwięcej podobnych stron lub aplikacji oraz poznać aktualne trendy i technologie. Po trzecie trzeba jak najszybciej zacząć testować swój projekt z użytkownikami, aby poznać ich opinie i poprawić projekt.

Warto też pamiętać, że obecnie standardem jest projektowanie responsywnych stron www, czyli takich, które dopasowują się do różnych urządzeń. My jako projektanci powinniśmy więc zaprojektować wygląd, układ i działanie interfejsu zarówno z myślą o ekranie komputera, jak i tabletu czy smartfona.

Więcej o projektowaniu responsywnych stron www:
https://it-develop.pl/blog/co-to-jest-responsywna-strona-www.html

PROJEKTOWANIE STRONY WWW I APLIKACJI KROK PO KROKU

Jak zabrać się do projektowania strony www lub aplikacji?

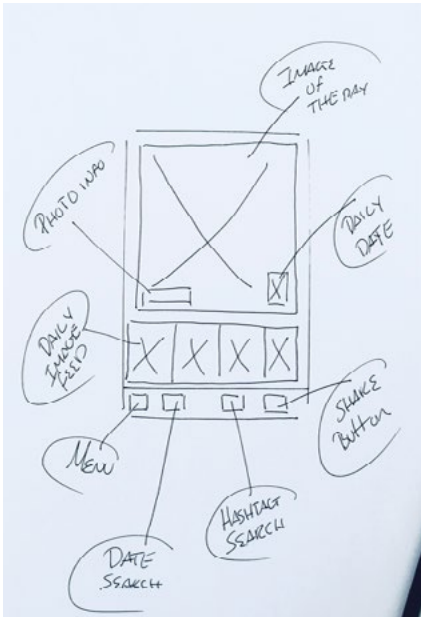
Najpierw oczywiście warto mieć pomysł na stronę lub aplikację i określić, kim będzie jej użytkownik, odbiorca. Czy będzie to osoba młoda? Nastolatek, dziecko? A może dorosły?

Odpowiedź na to pytanie pomoże stworzyć projekt, z którego ta wybrana osoba (i jej podobne) będzie chciała korzystać, a my będziemy mieć większe szanse na sukces.

W drugim kroku warto określić potrzebne na stronie informacje, zastanowić się, co powinno się na znaleźć na stronie lub w aplikacji. Np. każda standardowa strona internetowa składa się z: nagłówka (tzw. header), stopki (footer), menu oraz zawartości (tekstów, grafik, filmów). Do strony można też dodać linki do mediów społecznościowych i multimedia.

Potem należy wykonać schematyczny, czarno-biały szkic strony głównej i 1-2 dodatkowych podstron, można w nim notować, pisać, poprawiać go. Następnie można wykonać ulepszony szkic z naniesionymi kolorami przycisków czy nagłówka. Na jego podstawie wykonuje się interaktywną makietę, przez którą można się przeklikać. Udaje ona działający program. Potem dopiero przechodzimy do tworzenie strony www.

Po każdym z opisanych powyżej kroków warto wykonać testy z użytkownikami, by jak najszybciej dowiedzieć się, czy idziemy w dobrą stronę i jeśli trzeba: wykonać szybkie poprawki w prototypie.



Źródło obrazka: https://dribbble.com/shots/4006131-App-project

Tak na przykład może wyglądać wstępny szkic strony. To ogólny zarys, tego co na niej widzimy. Możemy podpisać poszczególne elementy, zrobić notatki.

Można też ulepszyć swój szkic, narysować go powtórnie na kartce z większymi szczegółami, dodać kolory przycisków itd. W dalszym kroku możemy przenieść szkic stworzony na kartce do programu do tworzenia makiet.

Źródło obrazka: https://thedaylightstudio.com/blog/2015/03/19/wireframes-at-daylight

Ilustracja powyżej pokazuje szkic ekranu na kartce (po lewej stronie), a po prawej fragment makiety strony wykonany w programie do makietowania.

Makieta to graficzne przedstawienie podstawowych funkcji i układu elementów programu w formie szkicu na kartce papieru lub też interaktywnych ekranów symulujących wybrane funkcje. Takie interaktywne makiety można tworzyć w programach takich jak Figma, Marvel, Balsamiq.

SZKICE EKRANÓW I MAKIETA

Szkicowanie ekranów jest bardzo ważnym etapem projektowania gry lub aplikacji i nie można go pomijać. Dlaczego? Przede wszystkim dlatego, że szkic jest łatwy do wykonania, a więc łatwy do zmiany i poprawy. Jego stworzenie nie wymaga dużo pracy, dzięki czemu nie jesteśmy do niego przywiązani, tak jak np. do gotowej strony lub aplikacji. Szkic pozwala na prezentację pomysłu i przetestowanie go z użytkownikami na bardzo wczesnym etapie projektowania, co uchroni nas przed kosztownymi błędami i zmianami na dalszych etapach pracy nad stroną lub aplikacją.

Więcej o tym, jak projektować UX można przeczytać w bezpłatnej publikacji pt. UX- Jak projektować dla użytkowników, wyd. Strefa Kursów 2015, dostępnej pod tym linkiem: **http://jjakiela.prz.edu.pl/psge/Do%20przeczytania/ebook_ux_jak_projektowac_dla_uzytkownikow.pdf**

TESTOWANIE

Gdy makieta strony lub aplikacji w formie szkicu lub schematu jest już gotowa warto ją przetestować. Na tak wczesnym etapie projektu najlepiej sprawdzają się wywiady z użytkownikami połączone z testem makiety np. w formie zadania dla użytkownika do wykonania lub prezentacji połączonej z zadawaniem pytań do makiety.

Warto je przeprowadzić z minimum 6 przedstawicielami grupy docelowej naszej strony www lub aplikacji.

Pytania jakie można zadać po prezentacji lub przetestowaniu przez użytkownika makiety, mogą być następujące:

1. Opowiedz o swoich wrażeniach - co sądzisz o tym projekcie?
2. Co Ci się najbardziej podoba w tym projekcie?

3. Co Ci się w nim nie podobało?
4. Co można dodać do tego projektu?
5. Czego jest za dużo?

PODSUMOWANIE TESTÓW

Gdy już wykonamy kilka testów możemy spróbować je podsumować. Zastanowić się:

- Co nie zostało zrozumiane lub się nie spodobało?
- Co zostało pozytywnie odebrane przez odbiorców?
- Jakie pojawiły się propozycje zmian i pomysły?

Potem możemy podjąć decyzje, co do tego, które opinie i uwagi odbiorców wziąć pod uwagę, np. które z zebranych informacji są najważniejsze, które sprawią, że pomysł odniesie sukces?

Należy wybrać te informacje zwrotne, do których chcemy się odnieść i na tej podstawie nanieść poprawki do makiety. Wcale nie trzeba uwzględniać wszystkich sugestii i uwag użytkowników.

Projektowanie gier

Gry zagościły już na dobre w naszym życiu codziennym. Gramy na komputerach, konsolach, smartfonach, w domu, w poczekalni, w sklepie, wspólnie, ze znajomymi i samodzielnie. Wielu młodych ludzi wiąże swoją przyszłość z branżą gier, szczególnie, że w Polsce dobrze się ona rozwija, a wiele polskich gier odniosło międzynarodowy sukces. Nim jednak zaczniemy projektować gry, warto odpowiedzieć sobie na pytanie, czym one są.

DEFINICJA GRY

Gra to najprościej rzecz ujmując rozrywka o ustalonych zasadach. Można też powiedzieć, że to aktywność, której uczestnik wykonuje działania zgodne z regułami, aby osiągnąć minimum jeden cel. Dobrze jest pamiętać, że gra nie musi wcale zawierać współzawodnictwa

i konfliktu; może polegać na tworzeniu, uczeniu się, poznawaniu, współpracy.

ELEMENTY, Z KTÓRYCH SKŁADA SIĘ GRA TO:

Granie – interaktywna rozrywka, w której uczestniczymy i możemy robić to sami.

Udawanie – przyjęcie umownych reguł i celu gry; rodzaj magicznego kręgu, w który wkraczamy decydując się na grę.

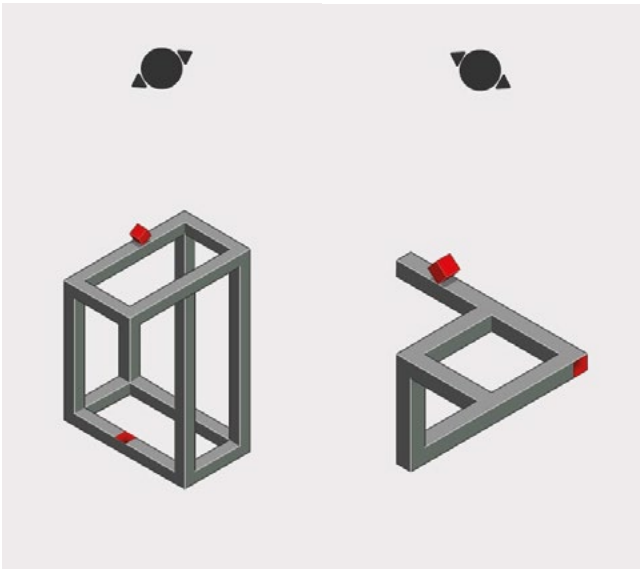
Cel gry – policzalny wynik (albo samo tworzenie), warunek zwycięstwa lub porażki, z lub bez rywalizacji; powinien być ciekawy, by gra była wyzwaniem oraz zdefiniowany przez reguły.

Reguły – definicje i instrukcje akceptowane przez gracza podczas gry, po wejściu do magicznego kręgu.

GATUNKI GIER

Istnieje wiele gatunków gier. Poniżej kilka najbardziej popularnych z przykładami bezpłatnych gier mobilnych na system Android, które możecie pobrać na swoje urządzenia i przetestować.

- Puzzle – np. Hocus, Alpha Bear, Memo, Kami 2, Lumosity, Dots
- RPG (role-playing game - czyli gra w pierwszej osobie) – np. InCell VR, Enigma Spy Adventure
- Symulacje (sportowe, pojazdów) – np. X Flight (bezpłatna gra mobilne)
- Wyścigi, przygodowe – np. Alto's Adventure, Sea Hero Quest (bezpłatne gry mobilne)
- Escape games (point-and-click) – np. There You Are (bezpłatna gra mobilna)
- Tap games – np. Axolotl Pet (bezpłatna gra mobilna)
- HOPA (hidden object puzzle adventure) – np. Detektyw Pozytywka (bezpłatna gra mobilna)
- Gry strategiczne (RTS) – np. Władca pierścieni: wyprawa do Śródziemia (bezpłatna gra mobilna)



Źródło obrazka: https://play.google.com/store/apps/details?id=air.com.gamebrain.hocus&hl=en

Powyżej screeny z bezpłatnej mobilnej gry logicznej Hocus.

Gry można podzielić także ze względu na sposób wykonania na:

- planszowe
- karciane
- cyfrowe: mobilne, webowe, komputerowe, oparte na VR lub AR, fizyce (akcelerometr, żyroskop), GPS, na połączeniu bluetooth, itd

Ze względu na tematykę dzielimy je na rozrywkowe i edukacyjne, które nie tylko stanowią rozrywkę, ale i przy okazji uczą, rozwijają wyobraźnię i np. logiczne myślenie. Przykładem takiej gry może być gra mobilna Cube Escape: Arles (Ucieczka z Arles) - rodzaj escape roomu, którego scenografią są obrazy Vincenta van Gogha.

Źródło obrazka: https://play.google.com/store/apps/details?id=air.com.RustyLake.CubeEscapeArles&hl=en

Powyżej screen z bezpłatnej gry mobilne Cube Escape: Arles.

Ćwiczenie:

znajdź w sklepie Google Play lub App Store i pobierz na swój smartfon lub iPhone jedną z wymienionych powyżej gier mobilnych. Wciel się w rolę testera: zagraj w grę i zastanów się co ci się w niej podobało, a co można by było poprawić w pierwszej kolejności? Czego było za dużo, a czego ci zabrakło? Jak można Twoim zdaniem ulepszyć grę?

ETAPY PROJEKTOWANIA GRY

Jak rozpocząć projektowanie gry? Tak jak i w przypadku projektowania strony czy aplikacji na początku prócz wyobrażenia sobie samej gry, warto określić też osobę, dla której tę grę projektujemy. Czy jest to dziecko, czy dorosły? Jakie ma zainteresowania? Jakie marzenia i potrzeby? Tylko wtedy możemy stworzyć grę, która faktycznie ma szansę trafić do naszych odbiorców i odnieść sukces.

PROJEKTOWANIE BOHATERA GRY

Następnie, jeśli jest to gra typu RPG, czyli gra w pierwszej osobie, w której wcielamy się w postać, należy wymyślić bohatera gry. Zastanowić się, kim on jest, dlaczego to właśnie on miałby być bohaterem, co w nim takiego jest, co sprawi, że odbiorcy zechcą się w niego wcielić? Jakie są jego mocne strony: co potrafi, co umie, co wie? Jakie są jego słabe strony: z czym sobie nie radzi, co sprawia jej/jemu trudność?

Inspiracji możesz szukać w znanych ci grach, książkach i filmach, np. tych wytwórni Pixar: ToyStory, Gdzie jest Dory, Iniemamocni, Potwory i spółka. Filmy te są tak popularne, ponieważ ich bohaterowie są bardzo ludzcy, mimo tego, że czasami są postaciami zupełnie wymyślonymi, zwierzętami lub fantazyjnymi stworami. Mają i słabe i mocne strony, nie są tylko odważni lub też tylko strachliwi, ponieważ - wg twórców z wytwórni Pixat - bardziej podziwia się bohatera za jego starania niż za sukcesy. Dlatego bohater nie musi być ideałem, któremu wszystko się udaje.

Źródło obrazka: https://pixune.com/portfolio/character-drawing-sketch/

Przykłady szkiców postaci do gry.

Ćwiczenie:

przypomnij sobie postać swojego ulubionego bohatera filmowego. Jaki on jest? jakie są jego cechy? Mocne i słabe strony? Co go motywuje? Czego chce? Jakie jego cechy mógłby mieć bohater Twojej gry?

PROJEKTOWANIE SCENARIUSZA GRY

Gdy już opiszesz swojego bohatera, nadasz mu imię, wymyślisz jak wygląda, ile ma lat, gdzie miesza, jak wygląda jego otoczenie, możesz przejść do kolejnego kroku, którym jest wymyślenie sposobu, w jaki gra działa, jej celu, reguł, a w przypadku gier RPG: scenariusza gry, czyli przebiegu całej rozgrywki, historii, która za nią stoi.

Może zainspiruje Cię schemat opowiadania historii, stosowanym w wytwórni Pixar. Jest on następujący:

1. Dawno dawno temu... (przedstawiamy bohatera, czas i miejsce akcji)
2. Każdego dnia... (pokazujemy życie codzienne bohatera)
3. Pewnego dnia... (zmiana, która zaszła, nietypowe wydarzenie)
4. Z tego powodu... (wprowadzamy przeszkody w jego życiu, pokazujemy konsekwencje zmiany)
5. Z tego powodu... (tutaj piętrzą się kolejne przeszkody)
6. Aż wreszcie... (tutaj następuje rozwiązanie historii, konkluzja)
7. Od tego czasu... (prezentujemy widzowi to, co się zmieniło w życiu bohatera)

Na podstawie tak zarysowanego scenariusza bardzo szybko można wyobrazić sobie historię bohatera od początku do końca, a także przygody, jakie mogą spotkać go w grze.

MECHANIKA GRY I REALIZACJA

Gdy masz już zarys scenariusza, możesz przejść do opisania mechaniki gry, czyli elementów, które składają się na grę: liczby postaci, sposobu zdobywania punktów lub zasobów, rodzaju misji itd.

Gdy już masz te wszystkie informacje możesz - tak jak w przypadku projektowania strony

www i aplikacji - stworzyć prototyp (pierwowzór) gry w formie szkiców na kartce lub interaktywnej, klikalnej makiety. Wszystkie te materiały pomogą Ci przekazać informacje o grze do zespołu, który ją wykona. Składa się on z projektantów, scenarzystów, dźwiękowców, grafików, muzyków, testerów, menedżerów, marketingowców.

Możesz też spróbować stworzyć ją samodzielne z pomocą dostępnych programów. W sieci można znaleźć wiele serwisów i portali, które umożliwiają tworzenie gier zupełnie bez programowania (no-code) lub z minimalnym wykorzystaniem kodu (low-code).

Jednym z takich portali jest strona www.scratch.mit.edu, gdzie można zupełnie bezpłatnie stworzyć własną grę z pomocą klocków z poleceniami: np. idź w prawo, skręć w lewo itd. Podobnie działa program GameMaker Studio 2 (posiada on bezpłatną wersję próbną).

Przegląd 5 najlepszych programów do tworzenia gier:

- https://www.komputerswiat.pl/artykuly/redakcyjne/5-najlepszych-programow-do-tworzenia-gier/9g5xh3v

Rozszerzenie:

- https://gry.wp.pl/jak-stworzyc-gre-poradnik-dla-kazdego-kto-chce-zaczac-6502643446384769a

Publikacja gry

W internecie jest wiele miejsc, gdzie możesz opublikować swoją grę. Gry mobilne, czyli przeznaczone na smartfon, tablet, iPhone lub iPad można opublikować w sklepach Google Play i Apple Store. Gry komputerowe: na portalach Steam i itchi.io. Natomiast gry webowe: na portalu Kongregate.

GOOGLE PLAY

W sklepie Google Play można publikować i pobierać gry i aplikacje na urządzenia z systemem operacyjnym Android. **Google Play** to internetowy sklep z filmami, muzyką, książkami, aplikacjami i grami mobilnym, przeznaczonymi na system Android, na którym opartych jest większość używanych na świecie urządzeń mobilnych. W Google Play w 2019 roku było dostępne prawie 3 miliony gier i aplikacji. Podział zysków jest następujący 70% dla wydawcy lub twórcy gry, 30% dla sklepu.

Gra zatwierdzana jest przed publikacją i dopuszczeniem do sprzedaży przez zespół Google. Zarabiać można poprzez sprzedaż aplikacji, mikropłatności, zakupy w aplikacji (in-apps) i reklamy. Kto chce wydawać swoje gry w Google Play musi uiścić jednorazową opłatę wynoszącą $25.

APP STORE (APLIKACJE I GRY MOBILNE)

W sklepie firmy Apple App Store można publikować i pobierać gry i aplikacje na urządzenia z systemem operacyjnym iOS. Liczba gier i aplikacji w serwisie wynosi ponad 2,2 milionów. Podział zysków jest następujący 70% dla wydawcy lub twórcy gry, 30% dla sklepu.

Gra zatwierdzana jest przez zespół Apple. Zarabiać można poprzez sprzedaż aplikacji, mikropłatności, zakupy w aplikacji (in-apps) i reklamy. Kto chce wydawać swoje gry w Apple Store musi wykupić sobie konto developerskie za minimum $99 rocznie.

APP STORE (GRY I PROGRAMY KOMPUTEROWE)

W sklepie Apple można także publikować i pobierać gry i aplikacje na komputery MAC. Liczba gier i aplikacji w serwisie wynosi ponad 28 tysięcy. Podział zysków i wymagania dla wydawcy są podobne, co w przypadku publikacji aplikacji i gier mobilnych.

STEAM

Na platformie STEAM można publikować i pobierać gry na komputery z systemem Windows oraz na komputery MAC z systemem iOS. Gra zatwierdzana jest automatycznie po utworzeniu konta. Zaletą platformy jest duża liczba użytkowników.

Podobną, lecz mniej znaną i popularną od STEAM platformą jest itchio.io. Można na niej opublikować maksymalnie 20 gier.

KONGREGATE

Gry online, czyli takie, które działają w popularnych przeglądarkach takich jak Chrome, Firefox czy Safari, można publikować i pobierać na portalu Kongregate.

Podsumowanie: różne rodzaje i formaty gier mają swoje wady i zalety. Gry komputerowe i mobilne są dość kosztowne w produkcji, wymagają dużych nakładów pracy, w dodatku trzeba zachęcić użytkownika, aby pobrał grę na swoje urządzenie, co w przypadku urządzeń

mobilnych z dość ograniczonymi zasobami pamięci może być dość trudnym zadaniem. Gry webowe, w które można grać w przeglądarce są znów łatwiejsze w produkcji i łatwiej można zachęcić kogoś by w nie zagrał, jednak mniej można na nich zarobić.

PRZYGOTOWANIE DO PUBLIKACJI GRY

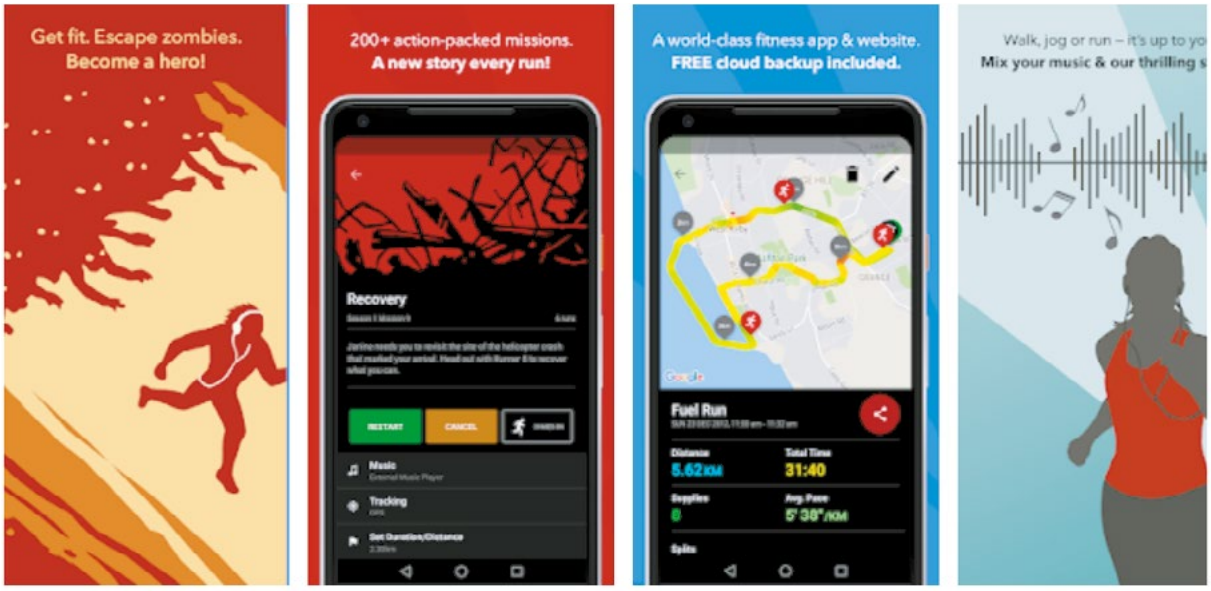
Do publikacji gry jest potrzebny plik z grą, np. w przypadku gier mobilnych Android plik .apk, który pobierzemy z programu, w którym tworzyliśmy grę. Przyda się także ikona gry oraz screeny z gry, czyli obrazki prezentujące interfejs gry. Do tego należy stworzyć krótki opis gry, zachęcający do jej pobrania oraz spis najważniejszych funkcji gry. W przypadku gier mobilnych musimy też wykupić konto developerskie (wydawcy) w jednym ze sklepów: Google Play lub App Store. Opcjonalnie: możemy stworzyć filmik prezentujący grę.

Projektowanie grywalizacji

Wszyscy lubimy grać w gry. Zauważyli to także edukatorzy, bankowcy, marketingowcy czy też firmy fitness. W wielu usługach i aplikacjach np. do nauki języków lub do biegania możemy zauważyć elementy znane nam z gier (punkty, nagrody, poziomy), których celem jest zaangażowanie uczestnika w różne, często nudne, ale bardzo potrzebne czynności, np. naukę, ćwiczenia fizyczne, czy też… co może być niebezpieczne - do częstszego płacenia przez internet. Takie działania nazywamy grywalizacją lub także gamifikacją (ang. gamification).

Przykładem zastosowania grywalizacji jest aplikacja Kahoot, która pomaga testować i powtarzać wiedzę w formie interaktywnych quizów, aplikacja Duolingo do nauki języków, mini-gra online pt. Kosmiczna podróż, która zachęca do nabywania wiedzy o kosmosie oraz popularna aplikacja Zombie run, której użytkownik biegając 'ucieka' przed zombie.

Przykład: aplikacja Zombie Run



Screeny z aplikacji Zombies Run (Google Play)

"Zombies, Run!" to jedna z wielu aplikacji motywujących do regularnej aktywności fizycznej – w tym przypadku do biegania. Wyróżnia się jednak na tle innych aplikacji, które polegają na mierzeniu sportowych wyników, zapisywaniu tras, stawianiu sobie coraz ambitniejszych celów i dzieleniu się informacjami o własnej formie ze znajomymi. W „Zombies, Run!" bieganie to… uciekanie przed zombie! Świetnie nagrana ścieżka dźwiękowa podczas biegu przypomina, że za Twoimi plecami czają się potwory, które za chwilę zjedzą Twój mózg. By się przed nimi bronić, musisz biegać coraz szybciej, a za otrzymane bonusy budujesz bazę chroniącą przed umarlakami. „Zombies, Run!" to genialny przykład wykorzystania zabawy do zwiększenia motywacji - fragment pochodzi z bezpłatnej publikacji pt. Grywalizacja w działaniu, wyd. Laboratorium EE, Fundacja Orange, Fundacja Gerere:
https://www.dkkadr.waw.pl/wp-content/uploads/2019/11/Grywalizacja_v13.pdf

Do projektowania grywalizacji przyda się znajomość ludzkich motywacji, czyli tego, co sprawia, że sięgamy po gry i tak chętnie w nie gramy. To np. rywalizacja z samym sobą lub z innymi, odkrywanie i ekscytacja z tym związana, zdobywanie punktów, nagród, zasobów, rozwijanie swoich umiejętności, ale także sama możliwość tworzenia, budowania czegoś.

Jak zaprojektować grywalizację? Najpierw warto określić problem, który chcemy rozwiązać z pomocą grywalizacji. Problem ten może wynikać z naszych obserwacji, np. dorośli rzadko segregują śmieci, uczniowie w szkole za mało rozmawiają ze sobą na żywo. Następnie warto zastanowić się co mogłoby zmotywować te osoby do zmiany swojego zachowania.

Np. przyznawanie zniżek, punktów do wymiany, dostęp do treści premium na platformie cyfrowej itd. Pozwoli to opisać, jak dokładnie będzie przebiegała grywalizacja. Co gracz (uczestnik) powinien zrobić, jaką misję lub zadanie wykonać, aby uzyskać punkty lub zasoby.

PODSUMOWANIE

Pamiętaj, że:

1. Grywalizacja to nie gra!
2. Grywalizacja to także nie konkurs, więc nagrody nie są tu najważniejsze.
3. Najważniejsze w grywalizacji jest zaangażowanie uczestnika, aby chciał powtarzać różne nudne i żmudne czynności wielokrotnie. Dlatego ważne jest to, aby w grywalizacji było coś więcej niż punkty, np. poczucie przynależności do grupy, możliwość zyskania uznania innych, pomoc innym.

Więcej o grywalizacji można przeczytać w bezpłatnej publikacji pt. Grywalizacja-zrób to sam (wyd. Fundacja Orange), który dostępny jest pod tym linkiem:

https://fundacja.orange.pl/files/user_files/user_upload/publikacje/grywalizacja_poradnik.pdf

lub w bezpłatnej publikacji pt. Grywalizacja w działaniu, wyd. Laboratorium EE, Fundacja Orange, Fundacja Gerere:

https://www.dkkadr.waw.pl/wp-content/uploads/2019/11/Grywalizacja_v13.pdf

Jak zabezpieczyć stronę i aplikację przed włamaniem i kradzieżą danych użytkowników?

ZASADY BEZPIECZEŃSTWA W INTERNECIE:

1. Staraj się unikać przekazywania poufnych informacji (np. haseł) pocztą elektroniczną, SMS-ami. Jeśli zależy Ci na zachowaniu poufności komunikacji, używaj systemu szyfrującego komunikację e-mailową.
2. Gdy to możliwe, korzystaj z protokołu https. Przy logowaniu i przesyłaniu danych

sprawdź, czy adres w przeglądarce zaczyna się od https i widnieje obok niego symbol kłódki. Zainstaluj w swojej przeglądarce wtyczkę „Https Everywhere", dzięki której z każdą odwiedzaną stroną, która ma taką opcję, automatycznie będziesz łączyć się przez protokół https.

3. Nie przesyłaj ważnych danych, gdy korzystasz z niezabezpieczonej sieci Wi-Fi. Staraj się w takiej sytuacji unikać logowania się; jeśli masz taką możliwość, wykorzystaj do tego swoją sieć dostępną w telefonie.

4. Wymyślaj trudne do odgadnięcia hasła; używaj różnych haseł do różnych usług i regularnie je zmieniaj. Chroń swoje hasła – nie udostępniaj ich innym, nie zapisuj w widocznym miejscu.

5. Zmień ustawienia przeglądarki tak, aby nie zapamiętywała haseł. Wyloguj się, kiedy skończysz korzystać z danej usługi.

6. Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe. Aktualizuj również inne programy, z których korzystasz i używaj najnowszych wersji przeglądarek internetowych.

7. Zabezpiecz hasłem (blokadą) dostęp do komputera, telefonu, tabletu. Szyfruj dane przechowywane na dysku.

JAK ZABEZPIECZYĆ STRONĘ PRZED ATAKIEM?

Aby serwer oraz sama strona były bezpieczne przestrzegaj tych **8 zasad**:

1. Korzystaj z komputera z zainstalowanym i aktualnym programem antywirusowym

2. Korzystaj wyłącznie z zabezpieczonej sieci Wi-Fi

3. Stosuj mocne hasła do każdej usługi, z której korzystasz (połączenie liter, liczb i znaków specjalnych)

4. Zawsze nadawaj unikalne loginy (unikaj nazw: admin, root, user, login…)

5. Korzystaj z aktualnych programów do obsługi kont FTP i nie zapisuj w nich haseł do serwera

6. Jeżeli korzystasz z systemów CMS (WordPress, Joomla, PrestaShop, Drupal…) to pamiętaj, aby regularnie aktualizować zarówno system jak i dodatki

7. Same systemy CMS i dodatki do nich pozyskuj wyłącznie z oficjalnych źródeł

8. Upewnij się, że Twój serwer nie pozwala na przeglądanie listy plików i katalogów

Jak tworzyć bezpieczne hasła?

- min. 20 znaków
- duże litery, małe litery, cyfry, znaki specjalne (najlepiej na zmianę)

Dobre praktyki zwiększające bezpieczeństwo w sieci:

- zmieniaj hasło co 30 dni
- nie podawaj hasła osobom trzecim
- w komputerze stosuj ochronę antywirusową i firewall
- nie podawaj hasła, korzystając z nieznanych komputerów lub sieci wi-fi.

Więcej informacji, wiedz i inspiracji na temat bezpieczeństwa w sieci:
https://cyfrowa-wyprawka.org/lekcje

JAK ZABEZPIECZYĆ STRONĘ WWW PRZED WŁAMANIEM I KRADZIEŻĄ DANYCH?

Opracowanie na podstawie: https://trybawaryjny.pl/jak-zabezpieczyc-strone/

Wyobraź sobie, że Twoja strona internetowa jest jak biuro Twojej firmy. Udostępniając ją w Internecie otwierasz główne drzwi do swojego biura. Większość odwiedzających wejdzie do wskazanych pomieszczeń i zachowa się tak, jakbyś tego od nich oczekiwał. Znajdą się jednak też tacy, którzy nie mają dobrych zamiarów – będą próbowali wejść do pomieszczeń przeznaczonych tylko dla personelu, otwierać szafki, przeglądać poufne dokumenty i ukraść coś, co ma dla nich jakąś wartość. Oczywiście w drzwiach takich pomieszczeń, jak i szafkach posiadasz zamki, **jednak** wśród niepowołanych gości znajdą się też tacy, którzy potrafią je otwierać bez klucza.

Tak właśnie wygląda serwer, na którym trzymasz swoją stronę internetową, z jedną zasadniczą różnicą: wirtualni włamywacze są niezwykle szybcy, anonimowi i trudni do wykrycia.

Mogą wykraść poufne dane Twojej firmy oraz Twoich klientów, złośliwie je usunąć lub zainstalować na serwerze narzędzia służące do kradzieży danych (loginów, haseł, numerów kart kredytowych) bez Twojej wiedzy. Powodów włamań na serwery jest wiele, efekt końcowy

zawsze ten sam – straty finansowe i popsuta reputacja Twojej firmy.

Czy to się zdarza często? Nie uwierzysz jak bardzo! Każdego dnia hackowane jest ponad 30 tysięcy stron internetowych.

W praktyce nie da się całkowicie zabezpieczyć przed atakami cyberprzestępców. Można jednak znacznie zmniejszyć ryzyko włamania się na Twoją stronę internetową.

Oto kilka porad, dzięki którym Twoja strona będzie bezpieczniejsza

- Hasła, loginy i jeszcze raz hasła
- Aktualizuj wszystko co da się aktualizować
- Nie chwal się tym, co masz
- Monitoruj swoją stronę internetową

HASŁA, LOGINY I JESZCZE RAZ HASŁA

To zabawne, że najstarsze i najprostsze ataki są nadal skuteczne. Są to ataki typu **brute force**, czyli wielokrotne wpisywanie różnych haseł tak długo, aż atakujący trafi na to właściwe. Statystycznie takie ataki odbywa się co 39 sekund.

Hackerzy nie używają tutaj przypadkowych ciągów znaków. W Internecie można znaleźć setki baz zawierających najczęściej używane hasła. Skąd się biorą takie bazy? To proste – istnieją serwisy o wątpliwej legalności, które publikują wrażliwe dane, wykradzione z wielu znanych jak i mniej znanych stron internetowych.

Są tam między innymi loginy i hasła z serwisów takich jak **linkedIn**, **gmail**, czy też znanych dużych polskich sklepów internetowych. W serwisie haveibeenpwned.com możesz sprawdzić w bezpieczny sposób, czy Twój adres mailowy nie znajduje się już na takiej liście. Takie hasła są później dekodowane i zliczane wszystkie te, które się powtarzają.

Na ich podstawie tworzony jest ranking. Jednym z najpopularniejszych haseł w Polsce jest d… słowo na 4 litery. Występuje pojedynczo lub powielone dwukrotnie. Co ciekawe takiego właśnie hasła używali pracownicy instytucji rządowych, z kontami mailowymi w domenie .gov.

Hasła typu „admin", „hasło", imię + rok , czy też zwykłe wyrazy ze słownika nie są żadnym zabezpieczeniem i zostaną złamane bardzo szybko. Aby uniemożliwić (a raczej ograniczyć)

ataki typu brute force warto założyć limit na ilość nieudanych logowań. To znacznie spowolni proces odgadywania hasła i mimo, że będzie to dalej możliwe stanie się na tyle nieskuteczne, że nie będzie opłacalne.

Przy nieudanej próbie zalogowania nie powinniśmy również informować czy niepoprawny jest login, czy też hasło – dzięki temu włamywacz nie będzie w stanie odkrywać prawidłowych loginów. Dlaczego? Tutaj znowu pojawia się stara i prosta sztuczka – nie trzeba być hackerem, aby pobrać bazę skradzionych maili i loginów. Jeżeli użytkownik używa tego samego hasła do wszystkich serwisów, z których korzysta i akurat ma konto w naszym serwisie wystarczy podać te wykradzione dane.

Jeżeli okażą się takie same – tutaj już niż nic nie poradzimy. Jeżeli jednak użytkownik użył innego hasła, atakujący nie będzie w stanie dowiedzieć się, czy użytkownik ma faktycznie konto w naszym serwisie. Kolejnym ważnym punktem jest reset hasła – należy pamiętać, że ta opcja jest dostępna dla każdego – nie tylko prawdziwego i uczciwego użytkownika naszego serwisu.

Gdy użytkownik chce zresetować hasło nie powinniśmy wysyłać nowego hasła mailowo – dużo lepszym rozwiązaniem jest link, dzięki któremu użytkownik będzie mógł ustalić nowe hasło już w naszym serwisie. Nie możemy również podczas resetu hasła informować, czy podany login lub mail był prawidłowy – to również idealny sposób do pozyskiwania loginów przez niepożądane osoby. Samo „jeżeli podałeś poprawne dane wyślemy Ci link" wystarczy.

AKTUALIZUJ WSZYSTKO CO DA SIĘ AKTUALIZOWAĆ

Twoja strona internetowa umieszczona jest na serwerze. Serwer posiada system operacyjny, na nim zainstalowane różnego rodzaju aplikacje serwerowe, php, bazę danych i na końcu tego wszystkiego Twoją aplikację. Aplikacja (strona internetowa) również składa się z innych modułów.

Większość rozwiązań stosowanych w internecie (zakładanie kont, wysyłka maili, edycja formularzy) jest elementem wspólnym dla każdego serwisu, dlatego bez sensu byłoby tworzenie tych rozwiązań dla każdego serwisu z osobna. To jak wymyślanie koła na nowo. Dlatego też programiści używają open sourceowych bibliotek i frameworków.

Są to gotowe rozwiązania, które można pobrać i zaadaptować do potrzeb serwisu. Dzięki temu programista może pewne rzeczy zrobić o wiele szybciej. Takie rozwiązanie ma jednak zasadniczą wadę – kod źródłowy tych rozwiązań jest publiczny, więc dostępny dla każdego.

Każdy z tych elementów – zarówno kod naszej strony internetowej, jak i wszystkie serwerowe aplikacje – jest w mniejszym lub większym stopniu podatny na ataki.

Jeżeli nie posiadasz serwera dedykowanego nie masz wpływu na aktualizacje części z tych rzeczy, jednak zawsze możesz pytać operatora hostingu, czy dba o aktualizacje. Masz za to wpływ na wszystkie moduły, z których składa się Twój serwis – szczególnie, jeżeli opiera się o opensourceowe rozwiązania (typu WordPress). Jest wielu etycznych hackerów, którzy łamią zabezpieczenia w ramach przeprowadzanych testów na zlecenie klientów lub po prostu „dla sportu".

Tacy testerzy natychmiast zgłaszają wykryte usterki do twórców oprogramowania. Twórcy reagują (czasem wolniej, czasem szybciej) na zgłoszenie, publikując poprawki, czyli aktualizacje. Wykryte luki często są dostępne publicznie i niewiele później pojawiają się tzw exploity, czyli gotowe rozwiązania, które wykorzystują te luki, aby włamać się na serwer.

Nieetyczni hackerzy wyszukują na §stronach podatnych na exploity w sposób automatyczny i zazwyczaj również w sposób automatyczny umieszczają na nich niebezpieczny kod. Każda strona internetowa – nawet Twoja – posiada średnio 30 luk, dzięki którym można włamać się na serwer. Jeżeli nie aktualizujesz wszystkiego na bieżąco, możesz stać się kolejną liczbą w statystyce.

NIE CHWAL SIĘ TYM, CO MASZ

Wyszukiwarki internetowe takie jak Google „przeklikują" zawartość Twojej strony i umieszczają ich kopię w swojej bazie, udostępniając je publicznie w wynikach wyszukiwań. Niestety kopiowane są często miejsca, które powinny być dostępne tylko dla administratorów strony. Jednym z takich miejsc może być logowanie do panelu administracyjnego Twojego serwisu. Powinniśmy blokować takie miejsca tak, aby nie mogły zostać zaindeksowane przez wyszukiwarkę. Umieszczenie takiego miejsca w pliku robots.txt nie jest najlepszym pomysłem – plik ten jest publicznie dostępny, więc może go przejrzeć każdy, dodatkowo nie wszystkie wyszukiwarki muszą go przestrzegać. Dużo lepiej jest zablokować niepożądanych gości za pomocą pliku **.htaccess** – zainteresowani znajdą dużo obszernych poradników na ten temat w Internecie.

Jeżeli nasz serwis jest oparty o rozwiązanie typu opensource warto jest ukryć takie informacje przed odwiedzającymi. Załóżmy, że nasza strona oparta jest o platformę WordPress – wtedy standardowo w stopce strony pojawi się dumny napis „Powered by WordPress".

Jeżeli poszukamy w Google zwrotu: blog kulinarny „Powered by WordPress.", znajdziemy listę blogów kulinarnych, które używają tego skryptu a ich właściciele nie specjalnie myślą o bezpieczeństwie.

Standardowy panel logowania administratora na platformie WordPress znajduje się w zakładce **/wp-admin/** – wystarczy do listy zwróconych przez Google adresów dokleić tą końcówkę i już stoimy przed drzwiami „tylko dla personelu", których w ogóle nie powinniśmy zobaczyć.

Nie myśl, że samo ukrycie pewnych miejsc przed wyszukiwarkami i prosta zmiana nazwy panelu logowania wystarczy. Istnieją specjalne aplikacje, które posiadają wbudowane bazy najpopularniejszych nazw plików i folderów, które mogą zwierać dane poufne i panele logowania.

Jedna z tych aplikacji posiada w swojej bazie ponad 170 tys takich nazw – jej nazwy celowo nie podaję. Aplikacja ta „dokleja" te nazwy do adresu Twojej strony i metodą „brute force" wyszukuje wszystkie te miejsca, które znajdzie. Zmiana z „wp-admin" na „admin" lub „administartor" kompletnie nic nie da. Aplikacja taka znajdzie ten adres w kilka sekund. Nazwa panelu administracyjnego powinna być skomplikowanym ciągiem znaków, podobnie jak hasło administratora.

MONITORUJ SWOJĄ STRONĘ INTERNETOWĄ

Wszystkie wymienione powyżej metody zwiększą bezpieczeństwo, jednak nie zagwarantują, że nasz serwis nie zostanie prędzej, czy później zhackowany. Warto więc również zmienić koncepcję – załóżmy, że kiedyś zostaniemy zhackowani i starajmy się wykryć to jak najszybciej, aby móc usunąć wszystkie szkody, zanim będzie za późno. Tutaj z pomocą przychodzi serwis **web-utils.pl**, który zajmuje się monitoringiem dostępności oraz treści strony.

Serwis ten zapisuje treść naszej strony w swojej bazie i nieustannie porównuje zapisaną kopię z obecną stroną. Jeżeli treść strony lub część jej kodu ulegnie zmianie narzędzie wykryje to i niezwłocznie poinformuje nas za pomocą smsa. Jeżeli treść naszej strony lub niektóre jej elementy są dynamiczne i często się zmieniają serwis również sobie z tym poradzi, rozróżniając, które elementy zmieniają się regularnie a które pojawiły się wbrew intencji właściciela monitorowanej strony.

Na dodatek nie potrzeba żadnej specjalistycznej wiedzy, aby odpowiednio skonfigurować

narzędzie monitorujące – serwis dokonuje analizy naszej strony i sam automatycznie wybiera odpowiednie rozwiązania. To jeszcze nie wszystko – otrzymamy powiadomienie również o tym, że nasza strona została przekierowana na inny adres (częste sztuczki hackerów), serwer zwraca błąd lub strona jest po prostu niedostępna.

Otrzymamy również dostęp do szeregu ciekawych narzędzi oraz statystyk, które pozwolą nam sprawdzić, między innymi to, jak szybko ładuje się nasza strona dla odwiedzających z różnych krajów. Serwis web-utils.pl oferuje bezpłatny okres demo, sama cena również nie jest wygórowana w porównaniu do jego możliwości. Połączenie tego serwisu z regularnym robieniem kopii zapasowych strony, może uchronić nas przed wieloma problemami w przyszłości.

Aby sprawdzić, czy Twoja strona nie została już zhackowana skorzystaj z tego darmowego narzędzia – jeżeli Twoja strona padła ofiarą hackerów i służy do wykradania danych lub zawiera inne szkodliwe oprogramowanie została już umieszczona na czarnych listach, które ten serwis skutecznie sprawdzi.

Biblioteka pojęć:

Aplikacja mobilna

Program przeznaczony na urządzenia przenośne takie jak smartfon, tablet, iPad, iPhone; aplikacją mobilną może być np. kalendarz, mapa, gra, klient poczty elektronicznej.

Aplikacje można podzielić na takie, które działają bez dostępu do Internetu (samodzielne) lub też takie, które wymagają do niego dostępu, aby poprawnie działać. W zależności od systemu, na jakim oparte jest dane urządzenie przenośne aplikacje mobilne można ze sklepów takich jak Google Play (system Android) lub App Store (iOS). Aplikacje mogą być darmowe lub płatne, część oferuje również możliwość dokupienia dodatkowych opcji lub funkcji poprzez tzw. in-appy, czyli zakupy w aplikacji. Zarówno darmowe jak i płatne aplikacje mogą zbierać od użytkownika dodatkowe dane, które mogą wykorzystywać do celów marketingowych lub też odsprzedawać je innym firmom i organizacjom, dlatego warto zwracać uwagę, do jakich funkcji urządzenia aplikacja żąda dostępu i czytać regulaminy.

Źródło: https://pl.wikipedia.org/wiki/Aplikacja_mobilna

Aplikacja internetowa (także webowa)

Pogram działający w przeglądarce, który nie wymaga instalacji na urządzenie przenośne lub komputer; aplikacją webową może być np. gra, klient poczty elektronicznej, aplikacja do nauki języków. Aplikacja, aby działać musi mieć dostęp do internetu, więc nie można korzystać z niej offline.

Źródło: https://pl.wikipedia.org/wiki/Aplikacja_internetowa

App Store

Sklep internetowy firmy Apple sprzedający gry i aplikacje mobilne i komputerowe na urządzenia z systemem iOS: IPhone'y, iPady, komputery MAC. Liczba gier i aplikacji w serwisie w 2019 roku wyniosła ponad 2,2 milionów. Zarabiać w sklepie można poprzez sprzedaż aplikacji, mikropłatności, zakupy w aplikacji (in-apps) i reklamy, sprzedaż pakietową aplikacji dla firm i szkół.

Źródło: https://pl.wikipedia.org/wiki/App_Store

Aplikacja komputerowa (program komputerowy)

Program działający na komputerze np. z systemem Windows (PC) lub iOS (Mac), który należy na nim zainstalować i nie jest on częścią systemu operacyjnego; aplikacją komputerową może być np. program graficzny, gra, klient poczty elektronicznej, aplikacja do nauki. Aplikacja komputerowa najczęściej może działać ofline, bez połączenia z komputerem.

Źródło: https://pl.wikipedia.org/wiki/Aplikacja_mobilna

Makieta

Model obszaru, budynku, przedmiotu w zmniejszonej skali lub też dekoracja filmowa lub teatralna. W przypadku projektowania oprogramowania makieta to rodzaj prototypu - graficzne przedstawienie podstawowych funkcji i układu elementów programu w formie szkicu na kartce papieru lub też interaktywnych ekranów symulujących wybrane funkcje. Takie interaktywne makiety można tworzyć w programach takich jak Figma, Marvel, Balsamiq.

Źródło: https://sjp.pwn.pl/slowniki/makieta.html

Strona internetowa, strona WWW (ang. web page)

Prezentowany w przeglądarce internetowej pod konkretnym adresem www zbiór uporządkowanych logicznie elementów (tekstów, grafik, filmów), połączonych ze sobą przez nawigację oraz linki (tzw. hiperłącza). Najczęściej tworzona obecnie z pomocą języków HTML5, CSS 3 i JavaScript.

Źródło: https://pl.wikipedia.org/wiki/Strona_internetowa

Hiperłącze (ang. hyperlink, inaczej: odnośnik, odsyłacz, link, hiperlink)

Odwołanie zamieszczone w dokumencie elektronicznym (tekstowym, graficznym, wideo, animacji, PDF, HTML), które prowadzi do innego dokumentu lub innego miejsca w danym dokumencie. Uaktywnienie hiperłącza może nastąpić poprzez kliknięcie lub najechanie kursorem na element, który nazywany jest kotwicą. Powoduje to wyświetlenie docelowej informacji. Hiperłącza są powszechnie używane na stronach internetowych.

Źródło: https://pl.wikipedia.org/wiki/Hiper%C5%82%C4%85cze

Internet

(Skrót od angielskich słów inter-network, dosłownie „między-sieć") – ogólnoświatowy system połączeń między komputerami, określany również jako sieć sieci. To także przestrzeń adresów IP przydzielonych hostom i serwerom połączonym za pomocą urządzeń sieciowych, (np. kart sieciowych, modemów komunikujących się za pomocą protokołu internetowego).

Źródło: https://pl.wikipedia.org/wiki/Internet

Serwer WWW

(Ang.) web server – program działający na serwerze internetowym, obsługujący żądania protokołu komunikacyjnego HTTP. Z serwerem WWW łączy się poprzez sieć komputerową, przeglądarka internetowa, będąca jego klientem, aby pobrać wskazaną stronę WWW. Serwer WWW może też korzystać z usług innego, równolegle działającego oprogramowania, np. MySQL i PHP, udostępniając wynikowe, dynamicznie utworzone strony WWW, wzbogacone danymi z bazy danych.

Źródło: https://pl.wikipedia.org/wiki/Serwer_WWW

Przeglądarka internetowa

(Ang. web browser) – program komputerowy lub na urządzenia mobilne służący do pobierania i wyświetlania stron internetowych. Pozwala odtwarzać pliki multimedialne, grać w gry online, często przy użyciu dodatków, zwanych "wtyczkami".

Źródło: https://pl.wikipedia.org/wiki/Przegl%C4%85darka_internetowa

Wyszukiwarka

(Ang. search engine) – program lub strona internetowa odnajdujący w Internecie informacje

według podanych przez użytkownika słów kluczowych.

Źródło: https://pl.wikipedia.org/wiki/Wyszukiwarka_internetowa

Responsywna strona internetowa

To strona www, której układ automatycznie dostosowuje się do wielkości ekranu urządzenia: komputera, tabletu, smartfona. Wyświetlane na ekranie treści zmieniają swój kształt i proporcje w taki sposób, by ich oglądanie było wygodne w odbiorze nawet na niewielkim urządzeniu.

Źródło: https://it-develop.pl/blog/co-to-jest-responsywna-strona-www.html

ARPANET

Pierwsza sieć rozległa oparta na rozproszonej architekturze i protokole TCP/IP. Jest bezpośrednim przodkiem Internetu. Istnieje do dziś.

Źródło: https://pl.wikipedia.org/wiki/ARPANET

Internet

(Ang.), inform. ogólnoświatowa sieć komputerowa, łącząca lokalne sieci, korzystające z pakietowego protokołu komunikacyjnego TCP/IP, mająca jednolite zasady adresowania i nazywania węzłów (komputerów włączonych do sieci) oraz protokoły udostępniania informacji. Stworzony w USA dla środowiska naukowego i akademickiego jako rozwinięcie sieci ARPANet (uruchomionej 1969), następnie rozszerzony na inne firmy i instytucje, od końca lat 90. stał się masowo dostępny także dla użytkowników (abonentów) indywidualnych.

Źródło: https://encyklopedia.pwn.pl/haslo/Internet;3915155.html

World Wide Web

(WWW) hipertekstowy, multimedialny, internetowy system informacyjny.

Źródło: https://pl.wikipedia.org/wiki/World_Wide_Web

Domena internetowa

Ciąg identyfikacyjny systemu Domain Name System (DNS), który określa zakres autonomii administracyjnej, uprawnień lub kontroli w Internecie. Nazwa domeny składa się z co najmniej jednej części, które (nazywane technicznie etykietami) są umieszczone w pewnym poddrzewie struktury DNS. Etykiety te są łączone i rozdzielane kropkami, np. example.com. Domena internetowa składa się z dwóch części - nazwy głównej oraz

końcówki - rozszerzenia. Nazwę główną bardzo często tworzy nazwa firmy/organizacji/akcji jej skrót bądź nazwa działalności, którą dana firma wykonuje. Rozszerzenie jest odgórnie ustalone - można wybrać spośród możliwych propozycji. Każdy kraj posiada przypisane rozszerzenie np. Polska - .pl, Rosja - .ru, Niemcy - .de, dla krajów Unii Europejskiej - .eu itd. Rozróżniamy domeny najwyższego poziomu: .com, .net, .org (zwane domenami globalnymi).

Źródło: https://pl.wikipedia.org/wiki/Domena_internetowa

Google Play

Internetowy sklep z filmami, muzyką, książkami, aplikacjami i grami mobilnym, przeznaczonymi na system Android, na którym oparte jest większość używanych na świecie urządzeń mobilnych. W Google Play w 2019 roku było dostępne prawie 3 miliony gier i aplikacji. Aplikacje mogą być darmowe lub płatne, część oferuje również możliwość dokupienia dodatkowych opcji lub funkcji poprzez tzw. in-appy, czyli zakupy w aplikacji. Sklep powstał w 2012 roku, po przekształceniu ze sklepu Android Market, założonego w 2008 roku i Google Music.

Źródło: https://pl.wikipedia.org/wiki/Google_Play

Hosting

Udostępnianie przez dostawcę usług internetowych zasobów serwerowni.

Innymi słowy, polega to na „zarezerwowaniu" (oddaniu do dyspozycji):

1. określonej objętości dysku twardego (zazwyczaj na macierzy RAID),
2. maksymalnej ilości danych do przesłania przez łącza internetowe serwerowni,
3. usług obsługiwanych przez serwerownię (w zakresie zależnym od specyfiki usługi, np. udostępnienie bazy danych z określeniem maksymalnej jej objętości),
4. maksymalnego stopnia obciążenia serwerowni przez usługi.

Źródło: https://pl.wikipedia.org/wiki/Hosting

Weebly

Serwis hostingowy z siedzibą w San Francisco. Jego firmą macierzystą jest Square, Inc. W momencie przejęcia w kwietniu 2018 roku, Weebly miał ponad 625.000 płatnych abonentów.

Źródło: https://en.wikipedia.org/wiki/Weebly

Wix

Kreator stron internetowych, który działa na światowym rynku od 2006 roku. Jest to najpopularniejszy na świecie kreator stron www. Często jego funkcjonalność jest porównywana z WordPressem, ponieważ oferuje szereg możliwości, których inne kreatory stron po prostu nie posiadają.

Źródło: https://www.pracawsieci.net/kreator-wix/

Blogger

Darmowy serwis blogowy stworzony w roku 1999 przez Pyra Labs a następnie przejęty i rozwijany przez Google w 2003. Zsynchronizowany z serwisem Picasa Web Albums. Blogi użytkowników widoczne są najczęściej w domenie blogspot.com.

Źródło: https://pl.wikipedia.org/wiki/Blogger

WordPress

Najpopularniejszy obecnie system zarządzania treścią (CMS), czyli witryna z wbudowanym panelem administracyjnym. To aplikacja, napisana w języku PHP, dzięki której można w prosty i intuicyjny sposób edytować swoją stronę internetową. Zaprojektowany głównie do obsługi blogów, ale nie tylko. Wykorzystuje bazę danych MySQL. Rozpowszechniany jest na licencji GNU General Public License i jest dostępny bezpłatnie. Według danych W3Techs, firmy analizującej rynek IT, w maju 2018 aż 30,7% stron na świecie pracowało w oparciu o Wordpress. Z kolei wśród systemów zarządzania treścią WordPress miał udział na poziomie 59,9% - czyli był najpopularniejszym CMS na świecie.

Źródło: https://pl.wikipedia.org/wiki/WordPress, https://hostclub.pl/co-to-jest-wordpress/

JavaScript

(W skrócie JS) – skryptowy język programowania, stworzony przez firmę Netscape, najczęściej stosowany na stronach internetowych.

Źródło: https://pl.wikipedia.org/wiki/JavaScript

PHP

Skryptowy język programowania zaprojektowany do generowania stron internetowych i budowania aplikacji webowych w czasie rzeczywistym. W roku 1997 język PHP/FI obsługiwało około 50 tysięcy domen internetowych. Do roku 2005 udział PHP rósł. Później uległ stabilizacji na poziomie ok. 20 milionów domen (9% wszystkich). Obecnie jest dominującym językiem programowania i obejmuje około 75% domen internetowych.

Źródło: https://pl.wikipedia.org/wiki/PHP

MySQL

Wolnodostępny, otwartoźródłowy system zarządzania relacyjnymi bazami danych, czyli zestaw programów służących do korzystania z bazy danych opartej na modelu relacyjnym. W najprostszym ujęciu w modelu relacyjnym dane grupowane są w relacje, które reprezentowane są przez tablice. Relacje są pewnym zbiorem rekordów o identycznej strukturze wewnętrznie powiązanych za pomocą związków zachodzących pomiędzy danymi. Relacje zgrupowane są w tzw. schematy bazy danych. Relacją może być tabela zawierająca dane teleadresowe pracowników, zaś schemat może zawierać wszystkie dane dotyczące firmy. Takie podejście w porównaniu do innych modeli danych ułatwia wprowadzanie zmian, zmniejsza możliwość pomyłek, ale dzieje się to kosztem wydajności.

Źródło: https://pl.wikipedia.org/wiki/MySQL

Blog

Rodzaj strony internetowej zawierającej odrębne, zazwyczaj uporządkowane chronologicznie wpisy. Blogi umożliwiają zazwyczaj archiwizację oraz kategoryzację i tagowanie wpisów, a także komentowanie notatek przez czytelników danego dziennika sieciowego. Ogół blogów traktowany jako medium komunikacyjne nosi nazwę blogosfery.

Źródło: https://pl.wikipedia.org/wiki/Blog

Vlog - Wideoblog

(Ang. videoblog, vlog lub vog) – rodzaj bloga internetowego, którego zasadniczą treść stanowią pliki filmowe (VODcast) publikowane przez autora w kolejności chronologicznej. Pliki udostępniane są do odtwarzania w technologii video-streamingu lub do pobrania na komputer użytkownika – gościa i widza wideobloga. Vlogerzy publikują swoje filmy głównie w serwisie YouTube oraz Dailymotion.

Źródło: https://pl.wikipedia.org/wiki/Wideoblog

Portal internetowy

Internetowy serwis informacyjny poszerzony o różnorodne funkcje internetowe, dostępny z jednego adresu internetowego. W intencji twórców ma to zachęcać użytkowników do ustawienia adresu portalu jako strony startowej w przeglądarce WWW i traktowania go jako bramy do Internetu.

Źródło: https://pl.wikipedia.org/wiki/Portal_internetowy

Forum dyskusyjne

Przeniesiona do struktury stron WWW forma grup dyskusyjnych, która służy do wymiany informacji i poglądów między osobami o podobnych zainteresowaniach przy użyciu przeglądarki internetowej. Fora dyskusyjne są współcześnie popularną formą grup dyskusyjnych w Internecie. Prowadzą je praktycznie wszystkie portale, większość wortali, znaczna liczba ISP. Są także powszechne na stronach wielu instytucji, czasopism, przedsiębiorstw, uczelni itp.; spotyka się również liczne fora zakładane prywatnie.

Źródło: https://pl.wikipedia.org/wiki/Forum_dyskusyjne

Serwis społecznościowy

Serwis internetowy, który służy do budowania sieci społecznych oraz stosunków społecznych, które opierają się na podobnych zainteresowaniach, wspólnym życiu zawodowym lub prywatnym. Umożliwia kontakt ze znajomymi oraz dzielenie się informacjami, zainteresowaniami.

Źródło: https://pl.wikipedia.org/wiki/Serwis_spo%C5%82eczno%C5%9Bciowy

Certyfikaty SSL

Są narzędziem zapewniającym ochronę witryn internetowych, a także gwarantem zachowania poufności danych przesyłanych drogą elektroniczną. Pełne bezpieczeństwo jest efektem zastosowania szyfrowania komunikacji pomiędzy komputerami. Certyfikaty SSL rejestrowane są na określoną nazwę domeny, zawierają informacje o właścicielu domeny, jego adresie itp. Dane te są zabezpieczone kryptograficznie i nie można ich samodzielnie zmienić.

Źródło: https://www.ssl.certum.pl/cert/certy_informacje_co_to_jest_certyfikat_ssl/

Protokół TLS

(Ang. Transport Layer Security) – przyjęte jako standard w Internecie rozwinięcie protokołu SSL (ang. Secure Socket Layer), zaprojektowanego pierwotnie przez Netscape Communications. TLS zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta. Opiera się na szyfrowaniu asymetrycznym oraz certyfikatach X.509.

Źródło: https://pl.wikipedia.org/wiki/Transport_Layer_Security

Ścieżka użytkownika

Droga jaką przebywa osoba odwiedzająca serwis, przechodząc pomiędzy stronami. W trakcie

analizy ścieżki należy brać pod uwagę nie tylko odwiedzane strony, ale również konkretne elementy

Źródło: https://westom.pl/zasady-tworzenia-sciezek-uzytkownikow/

Test 5 sekund

Jeden z najprostszych i najszybszych sposobów, który pomoże znaleźć błędy w stronie internetowej lub landing page. Podczas analizy wniosków pod uwagę brane są komunikaty werbalne (odpowiedzi na konkretne, zadane przez twórców pytania) i pozawerbalne (np. gesty i mimikę towarzyszącą oglądaniu strony). Za pomocą testu 5 sekund możemy sprawdzić między innymi czy użytkownicy wiedzą na jakiej stronie się znajdują?

Kevin Mitnick

Haker i autor, którego książka „Sztuka podstępu" ponad dekadę temu stała się bestsellerem w Polsce. Wydał także Sztukę infiltracji, opisującą prawdziwe ataki hakerskie oraz „Ducha sieci" – autobiografię obejmującą ok. 40 lat życia Mitnicka. Był osadzany w więzieniu dwukrotnie, najpierw w 1988 roku, a potem w latach 1995-2000. Został oskarżony o m.in. 14 przypadków oszust telekomunikacyjnych, 8 przypadków posiadania nieautoryzowanych urządzeń dostępów, nieautoryzowany dostęp do rządowego komputera.

Źródło: https://www.spyshop.pl/blog/10-najslawniejszych-hakerow/

Julian Paul Assange

Australijski aktywista internetowy, dziennikarz oraz programista, posiadający także obywatelstwo ekwadorskie, założyciel, rzecznik i redaktor naczelny serwisu WikiLeaks, witryny, która publikuje tajne informacje z osobistych kont internetowych, prasowych przecieków, poufnych dokumentów służb.

Źródło: https://www.spyshop.pl/blog/10-najslawniejszych-hakerow/, https://pl.wikipedia.org/wiki/Julian_Assange

Robert Tappan Morris

Amerykański informatyk, znany z napisania kodu pierwszego w Stanach Zjednoczonych robaka komputerowego. Jest synem szefa informatyków w National Security Agency. W 1988 r. był doktorantem na wydziale informatyki Uniwersytetu Cornell. Prowadził w tym czasie badania nad błędami w systemach 4 BSD Unix. Korzystając z wykrytych błędów napisał program nazywany dzisiaj robakiem Morrisa, który potrafił mnożyć się w tych systemach. Robak został uruchomiony 2 listopada 1988 r. Miał on mnożyć się w ograniczony sposób, jednak wskutek błędu programisty nie zadziałało wbudowane ograniczenie. Robak

w krótkim czasie praktycznie sparaliżował działanie ówczesnego, bardzo jeszcze skromnego Internetu zarażając ponad 6 tysięcy maszyn. Za swój czyn 22 stycznia 1990 r. został skazany na 3 lata obserwacji sądowej, grzywnę pieniężną 10 000 dolarów, 400 godzin prac społecznych i zapłacenie 150 000 dolarów kosztów postępowania sądowego. Obecnie jest profesorem Massachusetts Institute of Technology.

Źródło: https://pl.wikipedia.org/wiki/Robert_Tappan_Morris

Kevin Poulsen

Amerykański haker, spisał historię Maxa „Icemana" Butlera, słynnego m.in. z kradzieży milionów kart kredytowych, pt. Haker. Prawdziwa historia szefa cybermafii. Obecnie Poulsen jest jednym z redaktorów serwisu Wired. W 2006 roku pomógł policji złapać pedofila, który w 744 kontach na MySpace zamieszczał pornografię dziecięcą. W swojej historii udało mu się włamać do komputerów wielu znanych aktorek, Pentagonu, komputerów FBI. Ataki na komputery przeprowadzał w nocy. Swoje pierwsze oskarżenie o cracking usłyszał w 1989 roku. Zarzuty dotyczyły 19 przypadków oszustw, włamań do systemów telefonicznych i wyłudzenia pieniędzy. Udało mu się ukrywać przez 18 miesięcy przed zatrzymaniem. Wówczas udało mu się włamać do komputerów pewnego teleturnieju z radia KISS-FM w celu wygrania dwóch Porsche 944 w konkursie radiowym. W celu wygrania podszywał się pod nazwiskami Walter Kovacs oraz John Osterman.

Źródło: https://pl.wikipedia.org/wiki/Kevin_Poulsen

HTTPS Everywhere

Wtyczka do przeglądarek internetowych, która automatycznie włącza protokół HTTPS tam, gdzie istnieje taka możliwość.

Źródło: https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci#Slowniczek

Połączenie https://

Połączenie przeglądarki ze stroną internetową zapewniające szyfrowanie komunikacji, a tym samym znacznie utrudniające dostęp do treści osobom innym niż nadawca i odbiorca. Szyfrowanie niezbędne jest w bankowości elektronicznej i w innych sytuacjach, w których podajesz swoje prawdziwe dane. Korzystanie z połączenia https:// zaleca się każdorazowo przy logowaniu.

Źródło: https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci#Slowniczek

Protokół HTTP

(Ang. Hypertext Transfer Protocol) – jeden z podstawowych protokołów (tj. reguł postępowania i kroków podejmowanych przez urządzenie w celu nawiązania łączności i wymiany danych) Internetu, odpowiadający np. za ładowanie stron internetowych.

Źródło: https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci#Slowniczek

Protokół HTTPS

(Ang. Hypertext Transfer Protocol Secure) – rozszerzenie protokołu HTTP. Umożliwia przesyłanie w sieci zaszyfrowanych informacji, dzięki czemu dostęp do treści mają jedynie nadawca oraz odbiorca komunikatu.

Źródło: https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci#Slowniczek

Rozszerzenie (inaczej: wtyczka)

Dodatkowy moduł do programu komputerowego, który rozszerza jego możliwości. Stosowanie wtyczek jest coraz częstszym zabiegiem wśród programistów, a zwłaszcza tych tworzących otwarte oprogramowanie. Zaletą takiego rozwiązania jest to, że użytkownicy mogą wybierać pomiędzy funkcjami, które chcą mieć w programie, a których nie. Poza tym odciąża to autora od pisania całego kodu programu, a zrzuca część tego obowiązku na zewnętrznych programistów. Najpopularniejszymi programami oferującymi wtyczki są przeglądarki internetowe oraz programy pocztowe, np. Mozilla Firefox i Mozilla Thunderbird. W obu przypadkach dzięki wtyczkom można znacząco zwiększyć poziom bezpieczeństwa i prywatności komunikacji.

Źródło: https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci#Slowniczek

Gra

Rozrywka o ustalonych zasadach; aktywność, której uczestnik wykonuje działania zgodne z regułami, aby osiągnąć minimum jeden cel. Istnieje wiele gatunków gier, m.in. Puzzle, Gry strategiczne (RTS), RPG (role-playing game), Symulacje (sportowe, pojazdów), Wyścigi, przygodowe, Escape games (point-and-click), Tap games, HOPA (hidden object puzzle adventure). Gry można też podzielić ze względu na ich sposób wykonania lub użyte technologie: planszowe, karciane, komputerowe, mobilne, VR, AR.

Źrodło: https://pl.wikipedia.org/wiki/Gra

UX, user experience (doświadczenie użytkownika)

Wszystkie wrażenia, jakich doświadcza użytkownik podczas korzystania z usługi, produktu, strony www lub aplikacji. Obejmuje ono m.in. wygląd np. interfejsu (kolory, kształty, proporcje, czcionka), użyteczność (jak szybko użytkownik może zrobić to, czego potrzebuje), zawartość (teksty, multimedia)

Źródło: https://pl.wikipedia.org/wiki/User_experience

UI, user interface (interfejs użytkownika)

W informatyce: część oprogramowania, która umożliwia interakcje i porozumiewanie się z komputerem, aplikacją lub grą. Istnieje kilka rodzajów interfejsów: graficzne (GUI, graphic user interface), tekstowe (TUI, tekst user interface - wydajemy polecenia z pomocą tekstu) lub głosowe, które pozwalają na komunikację głosem. Najpopularniejsze obecnie interfejsy to interfejsy graficzne, jednakże coraz więcej pojawia się interfejsów głosowych lub umożliwiających komunikację gestem.

Źródło: https://pl.wikipedia.org/wiki/Interfejs_u%C5%BCytkownika

Scenariusz

Opis przebiegu (fabuły, narracji) filmu lub gry. Może zawierać dialogi, opis postaci, akcji, miejsca, czasu. Pozwala przekazać i przedstawić swoją koncepcję innym jeszcze przed przystąpieniem do jej realizacji.

Źródło: https://pl.wikipedia.org/wiki/Scenariusz

Użytkownik (ang. user)

Odbiorca, ktoś kto używa naszej strony, aplikacji lub też usługi czy produktu (rzeczy). Warto lepiej poznać jego zwyczaje i upodobania nim przystąpimy do tworzenia i realizacji naszego projektu, ponieważ wtedy projekt będzie dopasowany do jego potrzeb i mamy większą szansę na sukces.

Źródło: Podręcznik Design Thinking w Kulturze, https://www.agnieszkakaim.eu/publikacje/

„Cookie" (ciasteczka)

Wszystkie technologie, które przechowują i wykorzystują informacje na urządzeniu, na którym korzystasz z naszych Usług, np. na komputerze, tablecie lub telefonie komórkowym. Używamy na przykład plików cookie typu HTTP, które są niewielkimi plikami danych (zazwyczaj składającymi się z cyfr i liter), które pobierasz, kiedy zaczynasz korzystać z naszych

Usług, i które pozwalają nam rozpoznać Twoje urządzenie. Używamy także technologii takich jak znaczniki pikselowe i pakiety oprogramowania osadzone w naszych aplikacjach.

Istnieją różne typu plików cookie, na przykład:

- Pliki cookie obsługiwane bezpośrednio przez Cisco („pliki cookie administratora") i pliki cookie obsługiwane w naszym imieniu, np. przez agencje reklamowe lub firmy analizujące dane („pliki cookie osób trzecich").
- Pliki cookie, które funkcjonują przez określony czas, w tym te, które funkcjonują jedynie do czasu zamknięcia przeglądarki (tzw. „sesyjne pliki cookie"). Są one automatycznie kasowane po zamknięciu przeglądarki. Inne pliki tego typu to „trwałe pliki cookie", które nie są kasowane po zamknięciu przeglądarki. Służą one np. do rozpoznania Twojego urządzenia, gdy znów włączysz przeglądarkę internetową.

Źródło: https://www.cisco.com/c/pl_pl/about/legal/adct.html

Uwierzytelnianie wielopoziomowe

Sposób zabezpieczenia oraz autoryzacji podczas logowania przed skorzystaniem z konta użytkownika przez niepowołane osoby poprzez zdobycie przez nią identyfikatora użytkownika i hasła uwierzytelniającego. Oprócz podania tych danych logowania, użytkownik musi (w kolejnych etapach) podać uzyskany kod lub frazę np. ze swojego przenośnego urządzenia internetowego (np. smartfon, tablet), poprzez przepisanie go z e-maila wysłanego przez serwis, na którym użytkownik próbuje się zalogować, czy też za pomocą specjalnej karty, linii papilarnych palca itp.

Źródło: https://pl.wikipedia.org/wiki/Uwierzytelnianie_wielopoziomowe

Hasła

Są jednym z podstawowych sposobów, w jaki możemy udowodnić, kim jesteśmy. Używając ich logujemy się do poczty elektronicznej, bankowości on-line, dokonujemy zakupów w sieci i uzyskujemy dostęp do urządzeń, takich jak laptop lub smartfon. Można powiedzieć, że w wielu przypadkach hasła są niczym klucze do naszego królestwa. W związku z tym, jeśli ktoś byłby w posiadaniu Twojego hasła, mógłby dokonać kradzieży Twojej tożsamości, transferu Twoich pieniędzy lub uzyskać dostęp do wszystkich Twoich prywatnych danych. Używanie silnych haseł jest niezbędne, aby chronić swoją tożsamość i swoje informacje. Dowiedzmy się, co sprawia, że hasło jest silne i jak bezpiecznie je stosować. Silne hasła Cyberprzestępcy opracowali wyspecjalizowane programy, które coraz lepiej potrafią odgadnąć, a mówiąc inaczej "złamać", hasła. To oznacza, że mogą oni wykraść Twoje hasła,

jeśli są one słabe albo łatwe do odgadnięcia. Nigdy nie należy używać łatwo dostępnych informacji tworząc hasła. Do takich informacji należą na przykład data urodzenia, imię zwierzątka lub cokolwiek, co można łatwo znaleźć na portalach społecznościowych lub wyszukać w Google. Zamiast tego, najlepszym sposobem na stworzenie silnego hasła jest użycie długiego hasła, które im więcej znaków zawiera, tym lepiej. Najlepiej zamiast używać jednego słowa, używać wielu słów, a nawet pełnych zdań.

Źródło: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201305_po.pdf

Zapora sieciowa

Jeden ze sposobów zabezpieczania sieci i systemów przed intruzami. Termin ten może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, na którego straży stoi. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz, tzn. sieci publicznych, Internetu, chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz. Często jest to komputer wyposażony w system operacyjny (np. Linux, BSD) z odpowiednim oprogramowaniem. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.

Najczęściej używanymi technikami obrony są:

- filtrowanie pakietów, czyli sprawdzanie pochodzenia pakietów i akceptowanie pożądanych,
- stosowanie algorytmów identyfikacji użytkownika (hasła, cyfrowe certyfikaty),
- zabezpieczanie programów obsługujących niektóre protokoły.

Bardzo ważną funkcją zapory sieciowej jest monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do dziennika (logu). Umożliwia to administratorowi wczesne dokonywanie zmian konfiguracji. Poprawnie skonfigurowana zapora powinna odeprzeć wszelkie znane typy ataków. Na zaporze można zdefiniować strefę ograniczonego zaufania – podsieć, która izoluje od wewnętrznej sieci lokalne serwery udostępniające usługi na zewnątrz.

Źródło: https://pl.wikipedia.org/wiki/Zapora_sieciowa

Wirus komputerowy

Jest programem lub fragmentem kodu, przedostaje się do komputera bez Twojej wiedzy lub pozwolenia. Niektóre wirusy są tylko irytujące, ale większość wirusów jest destrukcyjna

i przeznaczona do infekowania i przejęcia kontroli nad podatnymi systemami. Wirus może przenosić się między komputerami i sieciami poprzez kopiowanie się, podobnie jak wirus biologiczny przechodzi z osoby na osobę.

Wirusy są zwykle ukryte w powszechnie używanych programach, takich jak gry lub przeglądarki plików PDF, możesz też otrzymać zainfekowany plik w załączniku do wiadomości e-mail lub wraz z innym plikiem pobranym z Internetu. Jak tylko wejdziesz w interakcje z plikiem (uruchomisz program, klikniesz na załącznik lub otworzysz plik), wirus automatycznie się uruchomi. Kod może wtedy skopiować się do innych plików i dokonać zmian w Twoim komputerze.

Źródło: https://www.avast.com/pl-pl/c-computer-virus

Cross-site scripting (XSS)

Luka w zabezpieczeniu strony umożliwiająca hakerom umieszczenie szkodliwego skryptu na zaufanej stronie lub w zaufanej aplikacji, który powoduje zainstalowanie złośliwego oprogramowania w przeglądarkach użytkowników. Za pomocą tej techniki hakerzy raczej nie atakują ani nie przekierowują użytkowników, lecz po prostu przesyłają swoje złośliwe oprogramowanie dużej grupie osób.

Źródło: https://www.avast.com/pl-pl/c-xss

Malware

To różnego rodzaju szkodliwe programy, które usiłują zainfekować komputer lub urządzenie mobilne. Hakerzy wykorzystują malware do różnych celów — wykradania danych osobowych, haseł i pieniędzy oraz blokowania dostępu do urządzeń. Przed zagrożeniem typu malware można się uchronić, stosując odpowiednie zabezpieczenia.

Źródło: https://www.avast.com/pl-pl/c-malware

Spyware

To rodzaj złośliwego oprogramowania, które jest wykorzystywane przez hakerów do szpiegowania, aby zyskać dostęp do Twoich poufnych informacji, danych bankowych lub aktywności online. Pokażemy Ci, w jaki sposób możesz zabezpieczyć się przed szpiegowaniem.

Źródło: https://www.avast.com/pl-pl/c-spyware

Adware

To typ złośliwego oprogramowania bombardującego Cię niekończącymi się wyskakującymi oknami, które potencjalnie mogą być niebezpieczne dla Twojego urządzenia.

Źródło: https://www.avast.com/pl-pl/c-adware

Keylogger

Jest to rodzaj oprogramowania szpiegującego, które potajemnie rejestruje naciśnięcia klawiszy, więc złodzieje mogą uzyskać informacje o Twoim koncie, kartach kredytowych, nazwy użytkowników, hasła i inne dane osobowe.

Źródło: https://www.avast.com/pl-pl/c-keylogger

Sniffery

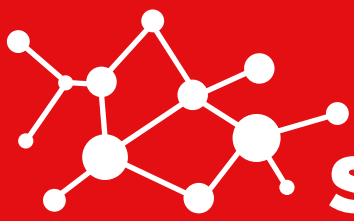
Przybierają różną postać. Są między innymi sniffery pakietowe, Wi-Fi, sieciowe czy IP. Wszystkie jednak mają jedną wspólną cechę – są to programy, które przechwytują wszystkie dane przepływające pomiędzy komputerem a siecią, z którą jest on połączony.

Źródło: https://www.avast.com/pl-pl/c-sniffer

Oprogramowanie ransomware

(Znane również pod nazwą rogueware lub scareware) - ogranicza dostęp do systemu komputerowego i wymaga zapłacenia okupu, aby blokada została usunięta. Najbardziej niebezpieczne ataki typu ransomware zostały spowodowane przez złośliwe oprogramowanie WannaCry, Petya, Cerber, Cryptolocker i Locky.

Źródło: https://www.avast.com/pl-pl/c-ransomware



sieć na kulturę

www.siecnakulture.pl

FUNDACJA **WSPIERANIA**
ZRÓWNOWAŻONEGO ROZWOJU