CHORY KOMPUTER, CZYLI RZECZ O WIRUSACH / ETYCZNI HAKERZY

10+ DLA DZIECI I DOROSŁYCH

NIE DAJ SIĘ CYBERZBÓJOM!

DLACZEGO WAŻNA JEST KOPIA BEZPIECZEŃSTWA

JAK ROZPOZNAĆ PHISHING

ZABEZPIECZAMY POCZTĘ GMAIL

ZNAJDŹ WIRTUALNĄ FLAGĘ

UŻYWAMY MANAGERA HASEŁ

CHRONIMY KONTA GAMINGOWE Z 2FA

JAK SKONFIGUROWAĆ ROUTER

UCZYMY SIĘ SZYFROWAĆ PLIKI

WSPÓŁPRACA

sekurak.pl

PROGRAMISTA JUNIOR

giganci programowania

bezpieczny.blog

NIE DAJ SIĘ CYBERZBÓJOM

Oddajemy w Wasze ręce niezwykłego e-booka poświęconego tematyce cyberbezpieczeństwa. Temat jest bardzo na czasie i jesteśmy przekonani, że materiały w nim zawarte pomogą w bezpiecznym korzystaniu z komputera i poruszaniu się po cyberprzestrzeni. E-book składa się z dziesięciu artykułów opublikowanych wcześniej na łamach magazynu *Programista Junior*, które są napisane bardzo przystępnym językiem, wypełnione wiedzą, przykładami oraz różnego rodzaju ciekawostkami. Publikacja skierowana jest do wszystkich osób, które skończyły przynajmniej dziesięć lat.

Podziękowania należą się przede wszystkim autorom, czyli **Gynvaelowi Coldwindowi**, **Marcinowi Gromkowi**, **Wiktorowi Szymańskiemu** i **Jarosławowi Jedynakowi**, których wiedza i lekkie pióro są nie do przecenienia. Nie można również zapomnieć o **Securitum Szkolenia**, **Gigantach Programowania** i osobach z **bezpiecznego bloga**, dzięki którym ten e-book powstał. Securitum Szkolenia to lider na rynku szkoleń związanych z bezpieczeństwem IT a Giganci Programowania to największa polska szkoła programowania dla dzieci.

Dzięki lekturze tej publikacji dowiecie się między innymi jak rozpoznać *phishing*, czyli jedną z najbardziej powszechnych metod ataków stosowanych przez cyberprzestępców. Poznacie metodę uwierzytelniania dwuskładnikowego (2FA) na przykładzie ochrony konta gamingowego, zabezpieczycie swoją skrzynkę e-mail oraz dowiecie się jak ważne jest używanie managera haseł.

Nauczycie się również szyfrować pliki, konfigurować własny router oraz dowiecie się dlaczego bardzo ważne jest tworzenie kopii bezpieczeństwa – o czym często zapominamy, a jest to rzecz która naprawdę pozwoli nam pozbyć się bólu głowy w wielu sytuacjach.

Na koniec dowiecie się więcej o zawodach *CTF* (co to jest i dlaczego to jest doskonała zabawa a jednocześnie forma nauki), wirusach komputerowych oraz... oraz obalimy niektóre mity dotyczące hackerów.

E-book nie wyczerpuje oczywiście tematyki związanej z cyberbezpieczeństwem, ale stanowi solidną podstawę. Zachęcamy do tego aby poszukiwać wiedzy dalej. Czy to na łamach pisma jak *Programista Junior*, portalach dotyczących bezpieczeństwa IT jak **Sekurak** czy też na zajęciach dla dzieci, które oferują Giganci Programowania.

Życzymy przyjemnej lektury. Przekażcie tę publikację dalej. Rodzinie, przyjaciołom, znajomym czy kolegom z klasy. Razem nie damy się cyberzbójom!

Łukasz Łopuszański
Redaktor prowadzący

Wprowadziliśmy wygodne oznaczenia do artykułów: kolor oraz wiek czytelnika. Zielony oznacza poziom łatwy, żółty poziom średni.

Artykuł dla prawie każdego, nie musisz posiadać specjalnych wiadomości, by zrozumieć treść. Poziom łatwy.

Musisz posiadać jakąś wiedzę w temacie, choć z lekką pomocą Internetu (może kolegów i koleżanek?) dasz radę! Poziom średni.

E-book „Nie daj się cyberzbójom" został przygotowany przez redakcję dwumiesięcznik Programista Junior, który jest wydawany jest przez Dom Wydawniczy Anna Adamczyk

Wydawca:
Anna Adamczyk
(annaadamczyk@programistajr.pl)
Redaktor prowadzący:
Łukasz Łopuszański
(llopuszanski@programistajr.pl)
Korekta:
Tomasz Łopuszański, Katarzyna Włodarczyk
Skład:
Krzysztof Kopciowski
Dział reklamy:
reklama@programistajr.pl
tel.: +48 663 220 102,
Prenumerata:
prenumerata@programistajr.pl

Adres wydawcy:
Dereniowa 4/47,
02-776 Warszawa
Strona internetowa:
www.programistajr.pl
Projekt okładki:
bok@keylight.com.pl
Współpraca:
Securitum Szkolenia Sp z o.o. Sk
(cyberzboj.sekurak.pl)
Giganci Programowania
(giganciprogramowania.edu.pl)
Bezpieczny Blog
(bezpieczny.blog)

NIE DAJ SIĘ CYBERZBÓJOM!

BEZPŁATNE

SZKOLENIE Z CYBERBEZPIECZEŃSTWA

14 WRZEŚNIA | **ON-LINE**

1 TERMIN
10:00-11:30

90 minut aktualnej, nieprezentowanej
nigdy wcześniej wiedzy!

2 TERMIN
20:00-21:30

PHISHING ▪ ATAKI GŁOSOWE ▪ NAMIERZANIE UKRYTYCH KAMER
RANSOMWARE ▪ BEZPIECZEŃSTWO W PODRÓŻY ▪ SESJA Q&A

sekurak.pl

ZAPISZ SIĘ NA: CYBERZBOJ.SEKURAK.PL

CHCESZ WIEDZIEĆ WIĘCEJ O PROGRAMOWANIU?

ZAPRENUMERUJ

PROGRAMISTA JUNIOR

CZYLI NAJLEPSZE PISMO DLA DZIECI W WIEKU 10+

HTTPS://PROGRAMISTAJR.PL/TYPY-PRENUMERATY/

Marcin Gromek

Jak rozpoznać phishing?

Przeglądasz Internet albo grasz w swoją ulubioną grę, gdy nagle dostajesz wiadomość e-mail od administratora serwisu gamingowego – coś jest nie tak z twoim kontem i zaraz zostanie usunięte na zawsze. Aby to sprawdzić i zapobiec nieszczęściu, szybko logujesz się, korzystając z linka umieszczonego w otrzymanej wiadomości. I już – właśnie padłeś/aś ofiarą phishingu.

10+

DOWIESZ SIĘ

- Co to jest „phishing".
- Jak rozpoznać phishing oraz jak się przed nim bronić.

POTRZEBNA WIEDZA

- Posiadanie konta e-mail.

CO TO JEST PHISHING?

Phishing to rodzaj oszustwa, w którym przestępca podszywa się pod osobę lub firmę, aby wyłudzić od ofiary informacje. Atakującemu może zależeć na uzyskaniu dostępu do poczty e-mail, serwisu gamingowego lub bankowości elektronicznej. Wykradzione w ten sposób informacje mogą służyć do podszycia się pod zaatakowanego w kolejnej fazie oszustwa. Na przykład dane osobowe, jak imię, nazwisko czy PESEL, mogą posłużyć do uzyskania dostępu do pozostałych kont w innych serwisach lub nawet wyłudzenia kredytu w banku na dane ofiary.

Atak ten wykorzystuje metodę manipulacji popularnie zwaną socjotechniką lub inżynierią społeczną (ang. *social engineering*). Polega ona na wykorzystaniu emocji, łatwowierności i braku wiedzy użytkownika, aby nakłonić go do podania swoich danych. Jest to tania i bardzo skuteczna metoda ataku – nie jest wymagana zaawansowana wiedza techniczna, a jedynie dobry pomysł, który można wykorzystać na masową skalę.

DLACZEGO PHISHING DZIAŁA?

Atakujący często opierają ataki phishingowe o stresujące sytuacje, równocześnie oferując użytkownikowi łatwe wyjście z zaistniałej sytuacji. Przykładem może być wiadomość e-mail od administratora konta w serwisie gamingowym. Wiadomość wygląda łudząco podobnie do tej prawdziwej – ma ten sam font, logo, wyrażenia i sposób komunikacji. Treść otrzymanej wiadomości jest często niepokojąca, na przykład jeśli użytkownik nie zaloguje się w ciągu kilku godzin do serwisu, jego konto zostanie trwale usunięte! Wiadomość zawiera link do strony logowania, prowadzi on jednak do fałszywej strony serwisu, która wygląda tak samo jak prawdziwa – na pierwszy rzut oka nie wzbudza podejrzeń. Po wpisaniu loginu i hasła na fałszywej stronie pojawia się błąd albo oczekiwanie na zalogowanie trwa bardzo długo – logowanie nie udaje się. Zniecierpliwiona ofiara może uznać, że pomyliła hasło lub otworzyć kolejną kartę przeglądarki internetowej i wpisać adres serwisu ręcznie. Po poprawnym zalogowaniu na prawdziwej stronie użytkownik sam utwierdza się w przekonaniu, że wszystko jest OK. Zamyka przeglądarkę i wraca do swoich spraw, nieświadomy, że przekazał dane do logowania oszustom.

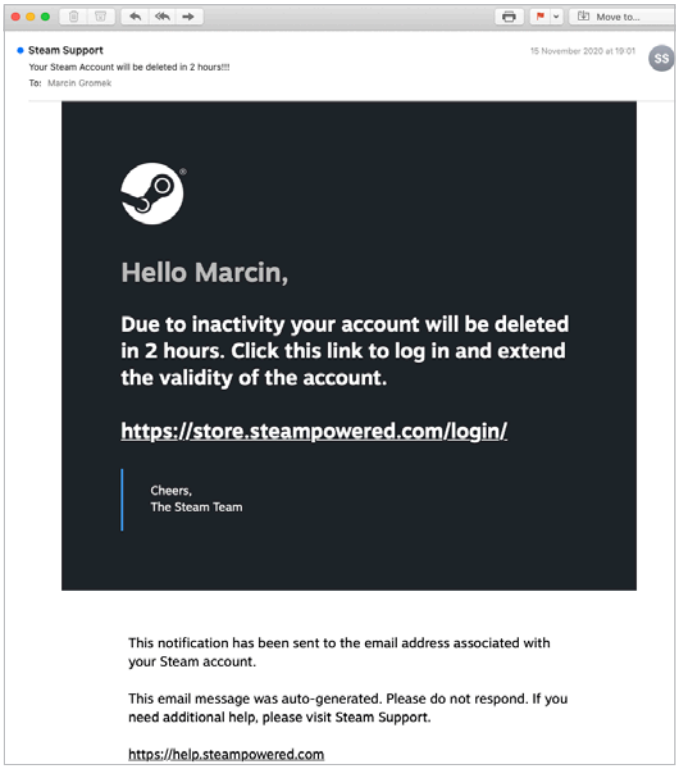
NA CO ZWRACAĆ UWAGĘ?

Wykonajmy ćwiczenie, w którym przyjrzymy się wiadomości phishingowej, widocznej na Ilustracji 1.

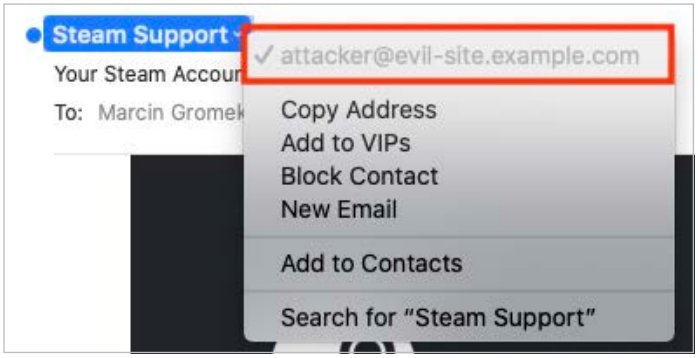
Wiadomość ta miała wyłudzić ode mnie dane logowania do serwisu gamingowego. Wykorzystuje ona wspomniany wcześniej scenariusz, w którym administrator serwisu gamingowego informuje użytkownika, że jego konto zostanie skasowane, jeżeli ten nie zaloguje się do serwisu w przeciągu kilku godzin. Uważny gracz, jeśli otrzyma taką korespondencję, powinien zwrócić uwagę na kilka szczegółów.

1. Adres nadawcy wiadomości

Prawdziwy adres nadawcy wiadomości e-mail często jest ukryty, a wyświetlana w kliencie pocztowym (program do odczytywania i wysyłania wiadomości e-mail) nazwa stanowi jedynie alias/nazwę ustawioną przez nadawcę w nagłówkach wiadomości. W ten sposób atakujący może wysłać wiadomość z adresu attacker@evil-site.com, a klient pocztowy ofiary wyświetli nazwę „Steam Support" zamiast pełnego adresu. Prawdziwy adres nadawcy można zobaczyć po kliknięciu w nazwę, jak przedstawiono to na Ilustracji 2 (zależy to jednak od wykorzystywanego klienta pocztowego).



Ilustracja 1. Przykład phishingowej wiadomości e-mail, podszywającej się pod serwis „Steam". Na pierwszy rzut oka wiadomość może nie wzbudzać podejrzeń



Ilustracja 2. Sprawdzanie faktycznego adresu e-mail nadawcy

2. Adres strony, do której prowadzi załączony link

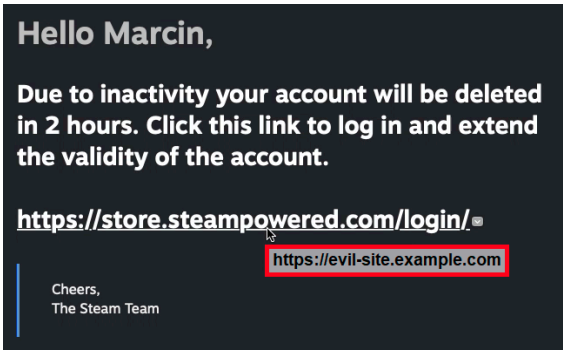
Wiadomość e-mail można stworzyć w tak zwanym „czystym tekście" (ang. *plain text*) lub przy użyciu języka HTML, który używany jest do tworzenia stron internetowych. Drugi sposób pozwala znacznie uatrakcyjnić wizualną stronę wiadomości, dlatego też często stosowany jest przez różnego rodzaju serwisy do korespondencji z użytkownikami. W języku HTML istnieje tag <a>, który pozwala na tworzenie linku (hiperłącza) ze słów w treści. Na przykład kod:

```
Due to inactivity your account will be deleted in
2 hours. Click this link to log in and extend the
validity of the account.

<a href="https://evil-site.example.com/">https://
store.steampowered.com/login/</a>
```

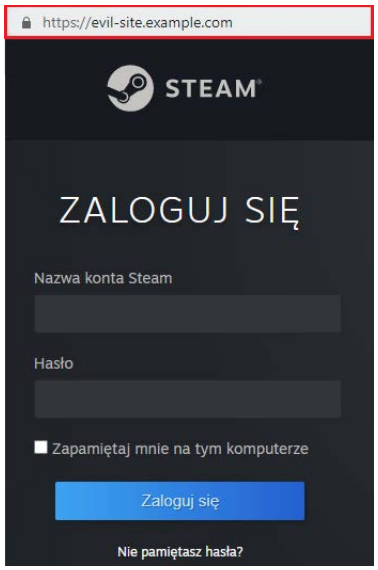
spowoduje wyświetlenie na stronie WWW lub w wiadomości e-mail słów „https://store.steampowered.com/login/" jako linku prowadzącego do strony „https://evil-site.example.com/". Jeśli klikniemy w taki odnośnik, zostaniemy przeniesieni na stronę, która została zdefiniowana w kodzie HTML (https://evil-site.example.com), a nie tę, która została wyświetlona użytkownikowi w treści wiadomości (https://store.steampowered.com/login/). Korzystając z tej techniki, atakujący może wyświetlić użytkownikowi dowolny adres lub tekst, a jednocześnie link może prowadzić na przykład do spreparowanej przez niego strony logowania serwisu Steam.

By zobaczyć prawdziwy adres, należy na niego najechać myszką. W zależności od używanego oprogramowania adres może się wyświetlić pod linkiem (Ilustracja 3) lub na przykład u dołu okna programu pocztowego.



Ilustracja 3. Pod linkiem kryje się zupełnie inny adres niż ten, który widać w treści wiadomości

Jeżeli kliknęliśmy w złośliwy odnośnik z wiadomości, adres fałszywej strony wyświetli się również w pasku adresu przeglądarki (Ilustracja 4). Na to również należy zwracać uwagę. W dzisiejszych czasach atakujący wykupują dla swoich stron certyfikaty SSL, więc to, że w przeglądarce przy adresie znajduje się kłódka, nie znaczy, że strona jest prawdziwa.



Ilustracja 4. Fałszywą stronę można rozpoznać po adresie URL znajdującym się w pasku adresu przeglądarki

3. Domeny podobne do prawdziwych

Czasem atakujący wykupują adresy domen bardzo podobne do prawdziwych, ale na przykład zawierające literówkę lub zamienione litery (adres „staem.com" zamiast „steam.com). Wykorzystują również fakt, że zestawy niektórych liter mogą wyglądać jak inna litera: na przykład litery „r" i „n" postawione jedna za drugą „rn" mogą przypominać literę „m". Ma to znaczenie, szczególnie gdy mamy do czynienia z małą wielkością tekstu (adres „stearn.com" może przypominać „steam.com"). Innym przypadkiem jest stosowanie małej litery „l" (L) jako dużej litery „i". To, czy litery będą skutecznie „udawać" inne znaki, zależy oczywiście od używanego fontu. Nazwa tego rodzaju oszustwa to *typosquatting*.

4. Błędy językowe

W samej treści często znajdują się literówki czy błędy gramatyczne. Nasz język nie jest łatwy do opanowania, a oszuści często używają tłumaczy online, jak na przykład Google Translate, które nie zawsze radzą sobie ze składnią, szczególnie pojedynczych zdań. Jeśli oszuści skorzystają z szablonu wiadomości e-maili w języku angielskim, a następnie przetłumaczą tekst na polski, mogą wyjść ciekawe fragmenty, na przykład:

- „Drogi Aleksandra" zamiast "„Droga Aleksandro" – w języku angielskim nie ma odmiany przez rodzaje.
- „Zostań w dotyku" zamiast „Pozostańmy w kontakcie" – dosłowne przetłumaczenie sformułowania „let's stay in touch".

JAK SIĘ BRONIĆ?

Przed zjawiskiem phishingu nie ma ucieczki, ale można się przed nim bronić, stosując się do kilku podstawowych zasad.

1. Wybierz sprawdzonego dostawcę poczty e-mail

Dostawcy usług pocztowych często stosują autorskie lub komercyjne systemy antyphishingowe. Moim zdaniem prym wiedzie poczta Gmail, która jednak osiąga to, analizując korespondencję swoich użytkowników. Bezpieczeństwo za prywatność.

2. Uruchom dwuskładnikowe uwierzytelnianie (2FA)

W artykule „Nie daj przestępcy ukraść swojego konta gamingowego" autorstwa Wiktora Szymańskiego możesz przeczytać o tym, czym jest dwuskładnikowe uwierzytelnianie i jak je uruchomić na platformie Epic Games. Proces włączania dwuskładnikowego uwierzytelniania w innych serwisach wygląda bardzo podobnie. W zależności od serwisu mogą być dostępne różne metody, na przykład kod z aplikacji mobilnej, klucz Yubikey czy kod dostarczany w wiadomości e-mail lub SMS.


Payment <kontakt@twojelogo.co.pl>
do kontakt

NETFLIX

ZAKTUALIZUJ SWOJE DANE

Cześć

Zaktualizuj swoje dane dotyczące płatności, aby kontynuować. Nie mogliśmy przetworzyć twojej ostatniej płatności. **Proszę zaktualizować dane dotyczące płatności**, aby móc nadal cieszyć się Netflix.

ZAKTUALIZUJ KONTO TERAZ

Postępuj zgodnie z poniższymi wskazówkami:

1. Zaloguj się na swoje konto. Tutaj.
2. Zaktualizuj swoje dane rozliczeniowe.
3. Zaktualizuj swoją metodę płatności.

Jeśli nie zweryfikujesz swojego konta, Twoje konto zostanie usunięte na stałe.
Pomóż nam wyczyścić swój status i odblokować konto.
Podziękowania

Zespół Netflix

Ilustracja 5. Przykład phishingowej wiadomości e-mail, która podszywa się pod serwis „Netflix" – na czerwono zaznaczone miejsca, na które użytkownik powinien zwrócić uwagę

3. Do wiadomości, które wzbudzają emocje, podchodź z rezerwą

To bardzo ważne! Jeśli otrzymujesz wiadomość, która wzbudza w tobie nagły przypływ emocji, to nie reaguj na nią pochopnie – przestępcy właśnie na to liczą. Podejmowanie decyzji w pośpiechu sprawia, że przestajemy zwracać uwagę na ważne szczegóły i znaki ostrzegawcze. Nic na szybko. Zanim klikniesz w link, poczekaj chwilę. Weź trzy głębokie wdechy i zastanów się nad treścią wiadomości. Ta dodatkowa chwila może uratować twoje konto i dane.

4. Loguj się z zapisanych wcześniej zakładek

Nawet jeżeli uważasz, że otrzymana wiadomość jest prawdziwa, to dla bezpieczeństwa nie loguj się do serwisu przez otrzymany w niej link, lecz wejdź na stronę poprzez zapisaną wcześniej zakładkę lub ręcznie wpisz adres strony w pasku adresu przeglądarki.

CIEKAWOSTKA

Nazwa „phishing" pochodzi od połączenia słów „password" – hasło i „fishing", czyli łowienie. Łącząc te słowa, mamy dosłownie „łowienie haseł". Wyraz „phishing" to homofon (wyraz identyczny fonetycznie, ale różny pod względem pisowni i znaczenia) do słowa „fishing". Po polsku czytamy „fiszing".

Marcin Gromek

Ekspert ds. bezpieczeństwa IT. Uwielbia słuchać podcastów i pić dobrą kawę. Pisze i nagrywa dla serwisu bezpieczny.blog.

KONTAKT@BEZPIECZNY.BLOG
HTTPS://BEZPIECZNY.BLOG

!

ZAPAMIĘTAJ

- „Phishing" wykorzystuje emocje i pośpiech ludzi. Jeśli otrzymana wiadomość wzbudza emocje, to daj sobie chwilę. Może to uratować twoje dane.
- Autorem wiadomości nie zawsze jest ten, kto jest podpisany na jej końcu.
- Oszuści wykorzystują też inne kanały komunikacji: telefon, SMS, Messenger, czy WhatsApp.

ĆWICZ W DOMU

- Przejdź kursy obrony przed phishingiem online.
- Istnieją interaktywne kursy, które mogą pomóc w nauce rozpoznawania złośliwych wiadomości, na przykład https://phishingquiz.withgoogle.com/.
- Podziel się zdobytą wiedzą z innymi. Nie dość, że ich uświadomisz i może nawet ochronisz, to dodatkowo lepiej przyswoisz zdobytą wiedzę.

Wiktor Szymański

Nie daj sobie ukraść konta gamingowego

Czyli co to jest 2FA

Budzisz się w sobotni poranek z myślą, że już niedługo zagrasz ze znajomymi w swoją ulubioną internetową grę multiplayer. Uruchamiasz komputer, próbujesz się zalogować, ale raz po raz otrzymujesz komunikat o błędnym haśle. To dziwne – masz pewność, że wpisywane hasło jest poprawne. Tymczasem znajomi przesyłają ci wiadomość, że ktoś gra już w twoim imieniu. Twoje konto zostało zhakowane!

10+

DOWIESZ SIĘ

- Jak poprawić bezpieczeństwo swojego konta gamingowego.
- Czym jest dwuskładnikowe uwierzytelnianie i jak go używać.

POTRZEBNA WIEDZA

- Jak instalować aplikacje na telefon z App Store/Google Play.

DLACZEGO KTOŚ CHCIAŁ PRZEJĄĆ MOJE KONTO?

Niestety, czasami hakerzy uzyskują nieautoryzowany dostęp do konta gamingowego graczy i wykorzystują je do niecnych celów. Robią to głównie po to, by sprzedać przejęte konto innym osobom, które na przykład nie chcą poświęcać czasu na zdobywanie doświadczenia w grze lub zostały zbanowane z uczestnictwa w rozgrywkach. Zdarza się, że przestępcy włamują się na konta, bo chcą skorzystać z unikatowych przedmiotów lub skinów. Często też okazuje się, że po włamaniu na konto wartościowe przedmioty zebrane na profilu gracza zostają rozdane lub sprzedane. Wyjątkowy łup dla przestępców stanowią konta z podpiętą metodą płatności. Hakerzy nie tylko zyskują wtedy dostęp do gier, mogą również dokonywać zakupów w twoim imieniu.

SKĄD PRZESTĘPCY MAJĄ DANE LOGOWANIA DO MOJEGO KONTA GAMINGOWEGO?

Hasło do konta to sekret, którego powinieneś strzec jak oka w głowie. Stanowi łakomy kąsek dla przestępców i dowcipnisiów. Najczęstszymi błędami popełnianymi przez użytkowników są:

- ustawianie wszędzie tego samego hasła – jeśli hasło „wycieknie" z jednego serwisu internetowego, przestępcy mogą zyskać dostęp do wszystkich twoich kont;
- zapisywanie hasła w widocznych miejscach – ciekawskie spojrzenia szybko wyłapują pozostawione na widoku sekrety;
- dzielenie się hasłem z wieloma użytkownikami – w ten sposób tracisz kontrolę nad tym, gdzie dalej przekazane zostanie twoje hasło;
- ustawianie prostego hasła – nazwa drużyny piłkarskiej i rok jej założenia nie jest trudnym do odgadnięcia hasłem.

Przestępcy mogą stosować również różnego rodzaju sztuczki, starając się nakłonić ciebie do podania im hasła. Do najpopularniejszych należy *phishing*, czyli wysłanie maila, w którym przestępcy udają kogoś innego – na przykład administratora strony internetowej – i zachęcają do logowania się do fałszywej strony serwisu gamingowego.

Ilustracja 1. Darmowa emotka „Boogie Down" dla użytkowników z włączonym 2FA w „Epic Games" (źródło: https://www.epicgames.com)

JAK ZWIĘKSZYĆ BEZPIECZEŃSTWO MOJEGO KONTA GAMINGOWEGO?

Większość serwisów gamingowych (na przykład Steam, Battle.net, Origin) umożliwia włączenie tak zwanego dwuskładnikowego uwierzytelniania (ang. *Two factor authentication* – 2FA). Podczas logowania do konta z grami oprócz loginu i hasła gracz podaje dodatkowy składnik, na przykład jednorazowy kod (ang. *One Time Password* – OTP) wygenerowany przez aplikację mobilną lub otrzymany SMS-em lub e-mailem. Kod ten, w przeciwieństwie do hasła gracza, generowany jest „w czasie rzeczywistym" i zmienia się po upływie kilkudziesięciu sekund (na przykład co 60 sekund). Przestępca, który próbuje zhakować twoje konto, nawet jeśli zna login i hasło, nie może się zalogować bez znajomości jednorazowego kodu.

Pomyśl o tym jak o dodatkowym zamku do domowych drzwi wejściowych. Nie otworzą się one, jeżeli oprócz pasującego klucza nie przekażesz im również jednorazowego cyfrowego kodu znajdującego się na smartfonie twoim lub twoich rodziców lub opiekunów. Fajne, prawda?

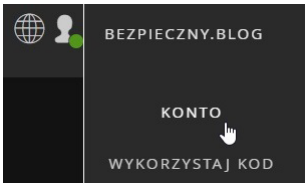
JAK WŁĄCZYĆ DWUSKŁADNIKOWE UWIERZYTELNIANIE NA KONCIE GAMINGOWYM?

W ramach ćwiczenia włączymy dwuskładnikowe uwierzytelnianie na platformie Epic Games. Masz konto w innym serwisie? Nic nie szkodzi! Proces włączania dwuskładnikowego uwierzytelniania w innych serwisach wygląda bardzo podobnie, dlatego po wykonaniu tego ćwiczenia na pewno poradzisz sobie również na innych stronach.

Zaloguj się na stronie https://www.epicgames.com. Na głównej stronie serwisu skieruj kursor myszy w prawy górny róg ekranu i przejdź do zakładki „KONTO".

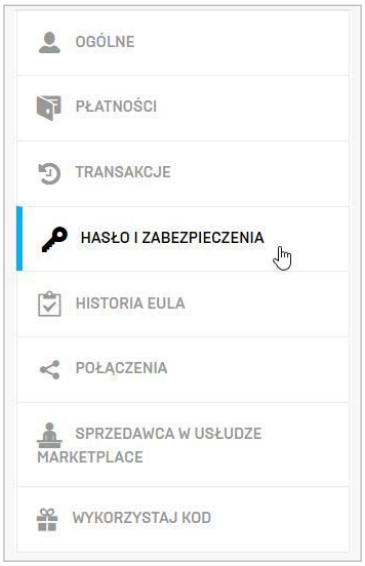
WARTO WIEDZIEĆ

Jeśli korzystasz z dwuskładnikowego uwierzytelniania w serwisie gamingowym i jednorazowy kod OTP przychodzi na twoją pocztę e-mail (taka możliwość dostępna jest między innymi w serwisie Steam), to koniecznie włącz dwuskładnikowe uwierzytelnienie również na swojej poczcie. Pamiętaj, by używać różnych haseł do konta pocztowego i serwisów gamingowych.



Ilustracja 2. Wybranie panelu ustawień konta

Wybierz zakładkę „HASŁO I ZABEZPIECZENIA" z panelu nawigacyjnego znajdującego się po lewej stronie.



Ilustracja 3. Wybranie ustawień bezpieczeństwa konta

Przewiń stronę do sekcji logowania dwuetapowego. Do wyboru mamy trzy opcje:

- APLIKACJA UWIERZYTELNIAJĄCA
- UWIERZYTELNIANIE WIADOMOŚCIĄ SMS
- UWIERZYTELNIANIE POPRZEZ E-MAIL

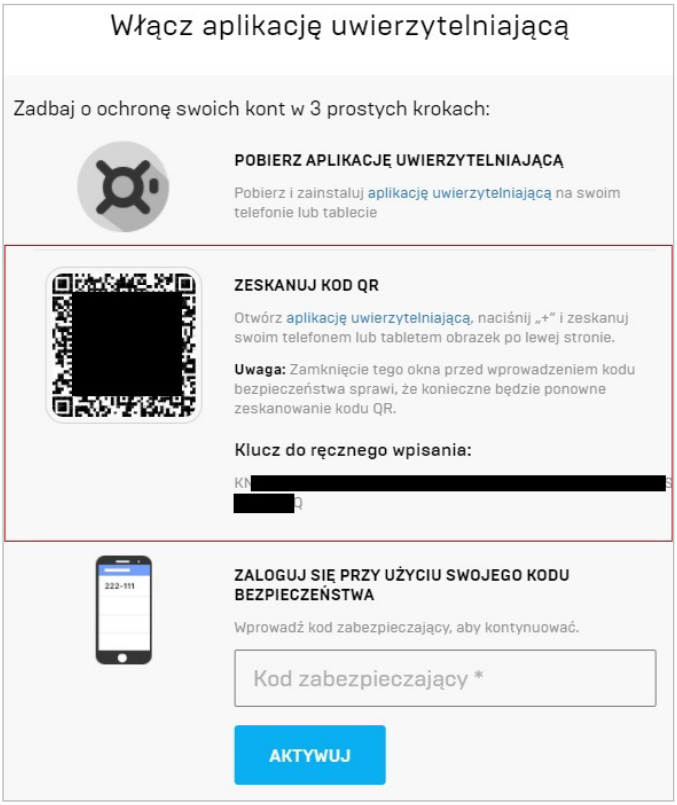
Jeżeli posiadasz smartfon i możliwość instalacji programów ze sklepu App Store/Google Play, rekomendujemy wybrać opcję „APLIKACJA UWIERZYTELNIAJĄCA". Na potrzeby tego ćwiczenia, jako aplikację uwierzytelniającą, wykorzystywał będę darmową aplikację *Google Authenticator* zainstalowaną na moim smartfonie.

CIEKAWOSTKA

Niektóre serwisy gamingowe nagradzają użytkowników za włączenie na koncie mechanizmów 2FA. Na przykład Epic Games udostępnia użytkownikom emotkę „Boogie Down" oraz daje dostęp do darmowych gier czy przedmiotów.

Ilustracja 4. Wybranie aplikacji uwierzytelniającej jako drugi składnik logowania

Następny ekran poprosi o uruchomienie na smartfonie aplikacji do dwuskładnikowego uwierzytelniania i sparowanie jej z kontem w serwisie Epic Games. Możesz to zrobić poprzez zeskanowanie kodu QR wewnątrz aplikacji lub ręczne wpisanie w telefonie klucza wyświetlonego na ekranie.



Ilustracja 5. Okno dodawania aplikacji mobilnej jako drugiego składnika logowania

Żeby zeskanować kod QR, uruchom aplikację do dwuskładnikowego uwierzytelniania na twoim smartfonie. Aby sparować urządzenie, naciśnij znak „+", a następnie wybierz jedną z dwóch dostępnych opcji: „Zeskanuj kod QR" lub „Wpisz klucz konfiguracyjny". Obie metody dają właściwie ten sam efekt, choć w kodzie QR może być zapisana dodatkowo nazwa serwisu, którego kod skanujesz. W mojej aplikacji *Google Authenticator* wyświetla się ona pod kodem OTP (jak na Ilustracji 7).

Ilustracja 6. Parowanie nowego konta z aplikacją mobilną „Google Authenticator"

Po wybraniu opcji skanowania kodu QR przytrzymaj obiektyw kamery przed kodem QR widocznym na ekranie komputera. Prawidłowo uchwycony kod QR wyświetli ekran z kodami OTP w aplikacji *Google Authenticator* (kody te są ważne tylko 30 sekund).

Ilustracja 7. Jednorazowy kod do serwisu „Epic Games" w „Google Authenticator"

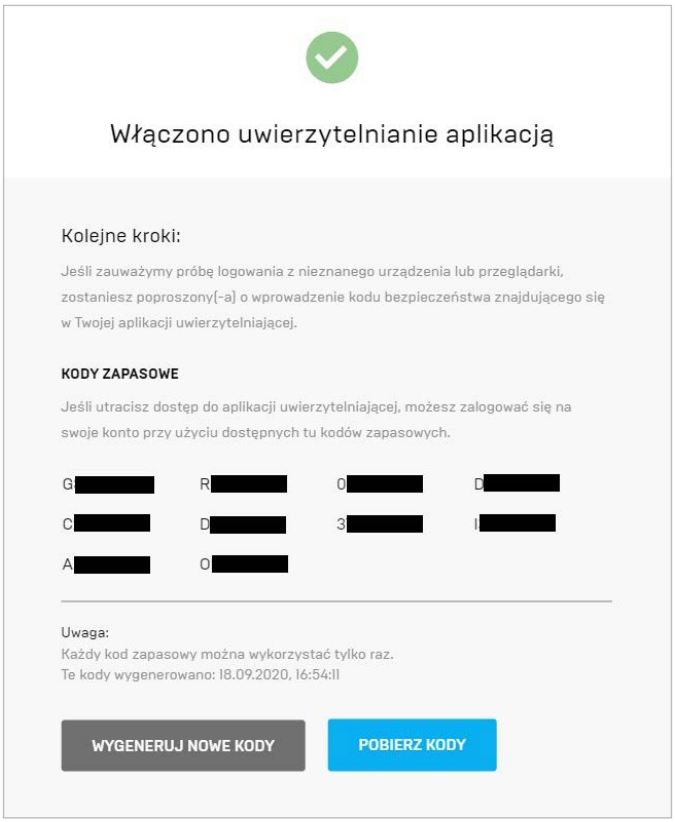
Wróć do ekranu serwisu Epic Games i przepisz swój jednorazowy kod, a następnie kliknij niebieski przycisk „AKTYWUJ".

Ilustracja 8. Miejsce przepisania kodu OTP z aplikacji mobilnej

Poprawne podanie kodu jednorazowego spowoduje wyświetlenie tablicy z kodami zapasowymi. Zapisz je w bezpiecznym miejscu na wypadek utraty dostępu do smartfona. Każdy kod możesz wykorzystać tylko raz. Dobrym zwyczajem jest wydrukowanie kodów i przechowywanie ich w bezpiecznym miejscu (na przykład książce, której nie wynosisz z domu).

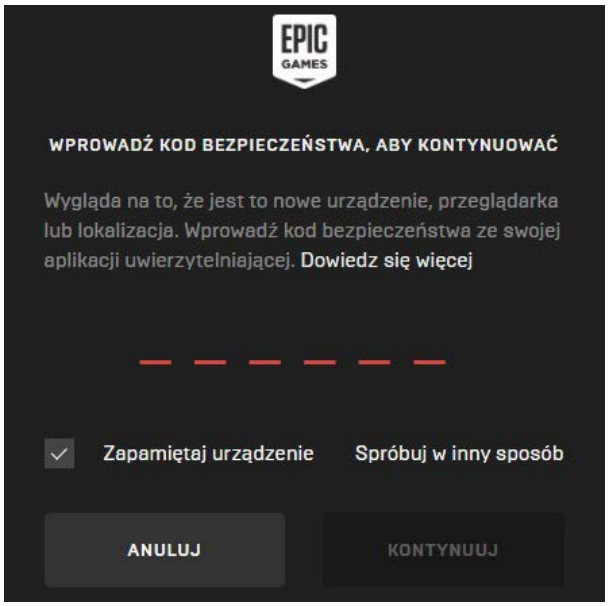
WARTO WIEDZIEĆ

Możesz użyć więcej niż jednej aplikacji do generowania kodów OTP. Jeśli boisz się, że twój smartfon się zgubi lub uszkodzi, w czasie włączania dwuskładnikowego uwierzytelniania poproś rodzica lub opiekuna o zainstalowanie aplikacji i zeskanowanie kodu QR lub wpisanie klucza konfiguracyjnego.



Ilustracja 9. Zapasowe kody OTP do zapisania jako kopia bezpieczeństwa

Od tego momentu dostępu do konta chroni dwuskładnikowe uwierzytelnianie. Możesz je przetestować, wylogowując się z konta i logując ponownie. Po wpisaniu prawidłowego loginu i hasła zostaniesz poproszony o podanie kodu z aplikacji mobilnej *Google Authenticator*. Jeżeli przy podawaniu kodu OTP zaznaczysz opcję „Zapamiętaj urządzenie", nie będziesz pytany/pytana więcej o kod OTP na urządzeniu, z którego właśnie się logujesz, będzie to jednak wymagane na każdym innym urządzeniu.



Ilustracja 10. Okienko wymagające kodu OTP przy logowaniu do konta

Wiktor Szymański

Współzałożyciel serwisu bezpieczny.blog, sympatyk dzielenia się wiedzą, maniak planszówek, miłośnik książek i filmów szpiegowskich. Na co dzień zajmuje się dbaniem o bezpieczeństwo aplikacji webowych.

KONTAKT@BEZPIECZNY.BLOG

ZAPAMIĘTAJ

- Zawsze dbaj o bezpieczeństwo swojego hasła.
- Dwuskładnikowe uwierzytelnianie podnosi bezpieczeństwo twoich kont w Internecie.
- Zrób kopię zapasową kodów przy parowaniu aplikacji mobilnej w procesie dwuskładnikowego uwierzytelniania.

ĆWICZ W DOMU

- 2FA możesz włączyć między innymi na takich platformach jak Steam, GoG, Battlenet, Epic Games.
- Włączenie dwuskładnikowego uwierzytelniania jest zalecane również w przypadku poczty e-mail oraz serwisów społecznościowych.

STACJONARNIE

ONLINE

giganci programowania

Zaprogramuj przyszłość swojego dziecka!

Szkoła programowania dla dzieci i młodzieży

SPRAWDŹ!

Zaufało nam **120.000** uczniów!

22 112 10 63

sekretariat@giganciprogramowania.edu.pl

www.giganciprogramowania.edu.pl

Wiktor Szymański

Jak zabezpieczyć pocztę Gmail?

Poczta elektroniczna (e-mail) to jedna z najpowszechniejszych form komunikacji w Internecie. Z roku na rok powiększa się grono osób preferujących wymianę informacji za pomocą mobilnych komunikatorów internetowych, jednak to właśnie posiadanie poczty e-mail jest często warunkiem koniecznym, by zarejestrować konto w większości portali internetowych (na przykład Netflix, Facebook czy Epic Games). Poczta elektroniczna jest też wykorzystywana jako podstawowy środek komunikacji w procesie resetu hasła użytkownika wielu serwisów. Warto zatem zadbać, by była bezpieczna.

12+

DOWIESZ SIĘ

- Dlaczego warto dbać o bezpieczeństwo poczty elektronicznej.
- Jakie mechanizmy bezpieczeństwa warto włączyć w swojej poczcie e-mail.

POTRZEBNA WIEDZA

- Posiadanie poczty e-mail.

DLACZEGO WARTO DBAĆ O BEZPIECZEŃSTWO POCZTY ELEKTRONICZNEJ

Włamania na skrzynki pocztowe to codzienność dla cyberprzestępców. Również tobie może przydarzyć się to, o czym do tej pory wyłącznie słyszałeś/aś od znajomych lub czytałeś/aś w Internecie. Czy tworząc konto poczty e-mail, ustawiłeś/aś jako hasło popularne słowo? A może w chwili nieuwagi kliknąłeś/aś na link prowadzący do fałszywej strony serwisu poczty elektronicznej? Te i wiele innych sytuacji mogą sprawić, że nieupoważnione osoby uzyskają dostęp do twojej poczty e-mail i zaczną przeglądać jej zawartość.

Przestępca, analizując historię twojej korespondencji elektronicznej, z powodzeniem może wytypować serwisy internetowe, w których założyłeś/aś konto, podając jako login swój adres e-mail. Tym samym może w tych serwisach skorzystać z procesu resetowania hasła, tak by zmienić je na wybrane przez siebie. Dzięki dostępowi do twojej skrzynki pocztowej nie będzie stanowiło to dla niego problemu, ty natomiast utracisz do nich dostęp, a wraz z nim wszystkie przechowywane tam informacje (dane, przedmioty, gry i tak dalej).

Skrzynka elektroniczna to nie tylko zbiór wiadomości wysyłanych do nas przez liczne serwisy internetowe. To także komunikacja wymieniana między tobą a różnymi instytucjami (szkołą, bankiem, pracodawcą), która w swojej treści (lub w załączniku) zawierać może cenne dla przestępców informacje. To również prywatne rozmowy ze znajomymi, które często chcielibyśmy zachować dla siebie. Im dłużej korzystamy z danego adresu e-mail, tym większa kolekcja rozmów i wrażliwych danych na nasz temat się w tej poczcie gromadzi.

Należy też pamiętać, że dostęp do konta e-mail użytkownika często otwiera przestępcy wrota do całego ekosystemu dostawców usług. Logując się do klienta pocztowego, użytkownik jest jednocześnie uwierzytelniany w kalendarzu, powiązanej usłudze do

przechowywania i synchronizacji plików[1] czy historii jego lokalizacji.

JAKIEGO DOSTAWCĘ POCZTY E-MAIL WYBRAĆ?

Istnieje wielu dostawców poczty elektronicznej. Jeżeli zaczynasz swoją przygodę z poruszaniem się po Internecie i nie czujesz się na siłach, by postawić i konfigurować swój własny serwer pocztowy, to proponuję założyć konto u jednego ze sprawdzonych dostawców poczty e-mail. Prywatnie rekomenduję pocztę Gmail, ponieważ:

- doskonale filtruje niechciane wiadomości – tak zwany SPAM,
- skutecznie identyfikuje ataki phishingowe[2] przeprowadzane na użytkowników,
- skanuje załączniki pod kątem wirusów i złośliwego oprogramowania,
- ma szereg mechanizmów, które możesz skonfigurować na swojej poczcie, by zwiększyć jej bezpieczeństwo (część z nich włączona jest domyślnie).

Gmail oczywiście nie jest jedynym dostawcą poczty, który oferuje takie możliwości, jest on jednak sprawdzony i polecany zarówno przez osoby techniczne, jak i nietechniczne. Po prostu działa.

O CZYM PAMIĘTAĆ, ZABEZPIECZAJĄC POCZTĘ

Kilka prostych zasad pozwoli nam zwiększyć bezpieczeństwo naszej elektronicznej skrzynki pocztowej:

1. Używaj silnego, unikalnego hasła[3]

O sile hasła decydują w głównej mierze dwa czynniki: jego długość i unikalność. Tworząc hasło do swojej poczty, zadbaj o to, by miało co najmniej 12 znaków i było na swój sposób „oryginalne". Krótkie hasła można złamać, stosując tak zwany atak siłowy (ang. *brute force attack*), który polega na sprawdzeniu każdej możliwej kombinacji znaków dla wybranej długości hasła. Jeżeli natomiast twoje hasło do serwisu internetowego to popularny zwrot, fraza lub ciąg znaków, to możesz być narażony na tak zwany atak słownikowy (ang. *dictionary attack*), w trakcie którego przestępca próbuje odgadnąć hasło do twojej poczty, korzystając z bazy popularnych, przygotowanych wcześniej, wyrażeń. Pod żadnym pozorem nie używaj tego samego hasła na innych stronach i w różnych aplikacjach. Gdybyś używał/a tych samych haseł i nastąpiłoby włamanie na jedno z twoich kont, przestępcy mogliby również zalogować się tym hasłem do twojej poczty.

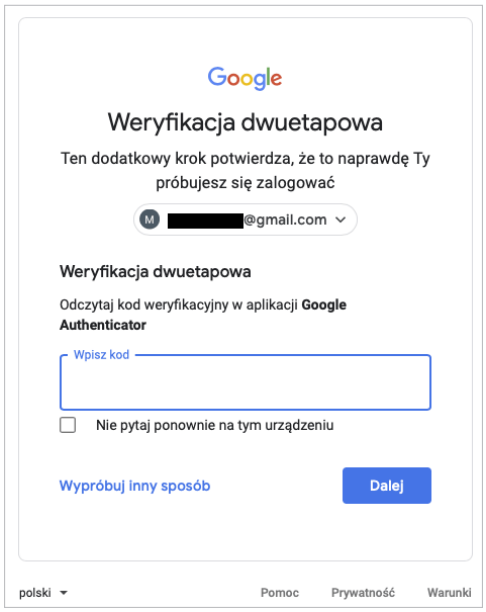
CIEKAWOSTKA

W Internecie można znaleźć bazy popularnych haseł wykorzystywanych przez użytkowników portali internetowych. Powstają one poprzez zebranie w jeden plik haseł, które wyciekły z serwisów, do których dokonano włamania. Przykładem takiej bazy jest zbiór o nazwie „RockYou": github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/rockyou-75.txt. Do najpopularniejszych haseł znajdujących się w tej bazie należą takie kombinacje jak: „123456", „Qwerty", „abc123", „Password" czy „iloveyou".

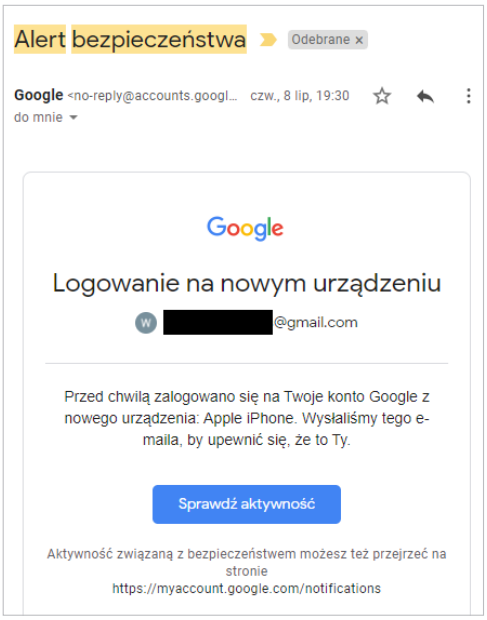
2. Uruchom weryfikację dwuetapową[4]

W artykule „Nie daj przestępcy ukraść swojego konta gamingowego" przeczytasz o tym, czym jest dwuskładnikowe uwierzytelnianie i jak uruchomić je na platformie Epic Games. Proces włączania dwuskładnikowego uwierzytelniania w innych serwisach wygląda bardzo podobnie. W zależności od serwisu mogą być dostępne różne metody, na przykład zapasowy kod bezpieczeństwa, powiadomienie „push" na telefon, kod z aplikacji mobilnej (Ilustracja 1), klucz Yubikey czy kod dostarczany w wiadomości e-mail lub SMS. Włączenie tego mechanizmu sprawi, że znajomość jedynie hasła do konta nie pozwoli atakującemu na uzyskanie dostępu do twojego konta. Informację, jak to zrobić w Gmail, znajdziesz na stronie www.google.com/landing/2step/.

1. Taką usługą może być na przykład dysk Google (ang. *Google Drive*), zobacz pl.wikipedia.org/wiki/Dysk_Google.
2. Zobacz artykuł „Jak rozpoznać phishing?".
3. W artykule „Używamy managera haseł" przeczytasz o metodzie tworzenia silnych haseł i generowania ich z wykorzystaniem programu KeePass.
4. Inaczej dwuskładnikowe uwierzytelnianie (ang. *two factor authentication* – 2FA).



Ilustracja 1. Formularz do wpisania jednorazowego kodu (ang. one-time password – OTP) wygenerowanego za pomocą aplikacji Google Authenticator do logowania na nasze konto



Ilustracja 2. Przykładowa wiadomość e-mail wysłana przez dostawcę usług pocztowych o tym, że uzyskano dostęp do skrzynki pocztowej z nowego urządzenia

3. Włącz powiadomienia bezpieczeństwa

Niektórzy dostawcy usług pocztowych pozwalają na włączenie funkcji informującej użytkownika (na przykład za pomocą wiadomości e-mail lub powiadomienia „push") o tym, że ktoś właśnie loguje się na konto z nieznanego wcześniej komputera lub urządzenia. Warto takie powiadomienia włączyć i dokładnie weryfikować tego typu ostrzeżenia. W poczcie Gmail funkcja ta jest domyślnie włączona (Ilustracja 2). Po zalogowaniu do poczty Gmail na stronie myaccount.google.com/notifications możesz sprawdzić wszystkie notyfikacje z ostatnich 28 dni.

WARTO WIEDZIEĆ

Przy włączonym mechanizmie weryfikacji dwuetapowej użytkownik będzie proszony o podanie jednorazowego kodu dostępowego przy każdym logowaniu do serwisu, chyba że zdecyduje się dodać urządzenie do zaufanych (w koncie google poprzez zaznaczenie okienka „Nie pytaj ponownie na tym urządzeniu" podczas wprowadzania kodu jednorazowego). W takim wypadku dla danego urządzenia (na przykład domowego komputera) zostanie stworzony wyjątek, ale mechanizm będzie aktywny dla wszystkich innych przypadków.

4. Szyfruj ważne dla ciebie informacje

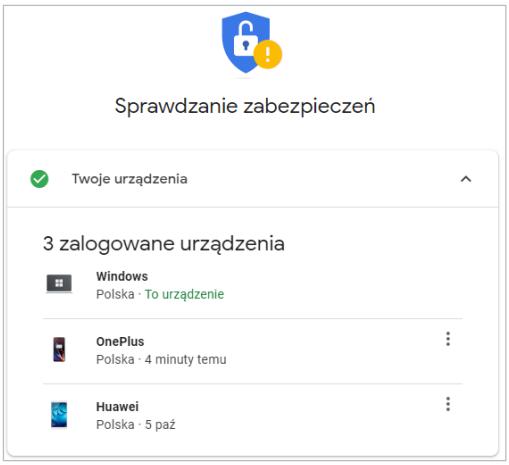
Pamiętaj, że nawet jeżeli ty dbasz o bezpieczeństwo swojej skrzynki, nie możesz być pewny poziomu bezpieczeństwa poczty osoby, z którą korespondujesz. Jeżeli przesyłasz dokumenty zawierające wrażliwe dla ciebie dane, zastanów się, czy nie warto zaszyfrować ich przed wysłaniem. Jeżeli przestępca uzyska dostęp do twojej skrzynki pocztowej lub skrzynki osoby, z którą korespondujesz, nie będzie mógł przeczytać informacji zawartych w pliku bez znajomości ustalonego przez ciebie hasła do zaszyfrowanych plików. Do szyfrowania samych załączników przed ich dodaniem do wiadomości e-mail możesz skorzystać z takich programów jak na przykład 7Zip (www.7-zip.org/). Jeżeli chcesz szyfrować całe wiadomości e-mail, skorzystaj z mechanizmu PGP/GPG dostępnego dla wybranego dostawcy usług pocztowych jako plugin do twojej przeglądarki.

5. Okresowo weryfikuj, jakie urządzenia mają dostęp do twojej poczty

Wiele serwisów pozwala na weryfikację, czy na dane konto ktoś (poza tobą) jest obecnie zalogowany. Co więcej, funkcja ta pozwala na „odłączenie" niechciane-

go urządzenia od twojego konta. Jeżeli okaże się, że na liście urządzeń znajdziesz takie, którego nie rozpoznajesz, usuń je, a następnie zmień hasło do poczty oraz włącz mechanizm dwuskładnikowego uwierzytelniania (jeśli jeszcze z niego nie korzystasz).

W poczcie Gmail informacje o tym, jakie urządzenia zalogowane są na twoją pocztę, sprawdzisz na stronie: myaccount.google.com/security-checkup.



Ilustracja 3. Widok zakładki „Twoje urządzenia" na stronie „Security checkup" w poczcie Gmail

6. Ustaw działanie na wypadek nieaktywności konta

Niektórzy dostawcy usług pocztowych pozwalają na zaplanowanie akcji, która wykona się w przypadku dłuższego okresu braku aktywności na skrzynce pocztowej. Jeżeli korzystasz z poczty Gmail, pod linkiem myaccount.google.com/inactive możesz wskazać okres czasu, po którym Google uzna twoje konto za nieaktywne, i zaplanować, co zrobić ze znajdującymi się na nim danymi. Masz możliwość udzielić dostęp do skrzynki pocztowej komuś zaufanemu lub poprosić o usunięcie znajdujących się na niej danych.

CIEKAWOSTKA

Większość dostawców poczty e-mail wymaga, aby użytkownik miał co najmniej 13 lat, by założyć internetowe konto pocztowe. W przypadku konta Google w Polsce wymagany jest wiek 16+. Jeżeli nie spełniasz tego wymogu, poproś rodziców lub opiekunów, żeby asystowali ci podczas zakładania konta.

PODSUMOWANIE

Dbając o nasze bezpieczeństwo w Internecie, powinniśmy przykładać szczególną wagę do bezpieczeństwa naszej poczty elektronicznej. Uzyskanie dostępu do naszej skrzynki pocztowej przez nieupoważnione osoby daje intruzom nie tylko możliwość czytania naszej korespondencji, lecz również umożliwia resetowanie haseł do powiązanych serwisów internetowych (Netflix, Facebook, Epic Games) i powiązanych z pocztą usług (na przykład Google Drive czy historii lokalizacji, jeśli mamy ją włączoną). Gorąco zachęcamy do zapoznania się ze wszystkimi funkcjami bezpieczeństwa konta Google pod adresem: myaccount.google.com/security.

Wiktor Szymański

Współzałożyciel serwisu bezpieczny.blog, sympatyk dzielenia się wiedzą, maniak planszówek, entuzjasta klocków LEGO, miłośnik książek i filmów szpiegowskich. Na co dzień zajmuje się dbaniem o bezpieczeństwo aplikacji webowych.

KONTAKT@BEZPIECZNY.BLOG
HTTPS://BEZPIECZNY.BLOG

ZAPAMIĘTAJ

- Ustaw silne, unikatowe hasło do swojej poczty.
- Włącz dwuskładnikowe uwierzytelnianie.

ĆWICZ W DOMU

- Wypróbuj różne narzędzia do dwuskładnikowego uwierzytelniania.
- Skonfiguruj powiadomienia bezpieczeństwa na swojej poczcie.

Wiktor Szymański

Używamy managera haseł

Według przeprowadzonego w 2020 roku badania przeciętny użytkownik Internetu wykorzystuje około 100 haseł, by logować się do mediów społecznościowych, sklepów internetowych czy serwisów streamingowych. Co zrobić, żeby zadbać o bezpieczeństwo haseł i się w nich nie pogubić?

12+

DOWIESZ SIĘ

- Co to jest manager haseł i jak z niego korzystać.
- Jak wygenerować losowe hasło.

POTRZEBNA WIEDZA

- Jak pobierać i instalować aplikacje na komputerze.

BEZPIECZEŃSTWO HASEŁ

Żyjemy w XXI wieku – odcisk palca daje możliwość zalogowania się do komputera, skan twarzy odblokowuje telefon, a barwa i ton głosu pozwalają na uwierzytelnienie klienta w trakcie rozmowy z konsultantem bankowości elektronicznej. To bardzo wygodne i powszechnie stosowane rozwiązania. Wiele osób zapomina jednak o tym, że jeżeli któraś z tych metod zawiedzie, dalej możliwe będzie skorzystanie z numeru PIN czy ustalonego wcześniej hasła, aby uzyskać dostęp do zasobów komputera, telefonu czy konta w banku. Dlatego ustawienie bezpiecznego hasła (a gdzie to możliwe - konfiguracja dwuskładnikowego uwierzytelniania) powinno stanowić priorytet dla każdego użytkownika Internetu.

Nowe wytyczne międzynarodowej organizacji związanej z bezpieczeństwem NIST (https://pages.nist.gov/800-63-3/sp800-63b.html#appA) zalecają korzystanie z jak najdłuższych haseł. To właśnie długość hasła jest ważniejsza od jego poziomu skomplikowania. Jak utworzyć silne i łatwe do zapamiętania hasło? Poniżej przykład:

1. Wymyśl sobie jakieś zdanie, które będzie dla ciebie łatwe do zapamiętania – na przykład „Mam dwanaście lat i mam dużego brata”.
2. Usuń spacje, polskie znaki, zamień słowo „dwanaście” na cyfrę i dodaj znak specjalny (na przykład „kropkę”) na końcu zdania. Otrzymasz hasło: „Mam12latimamduzegobrata.”. W tym momencie mamy 24-znakowe hasło, które zawiera w sobie duże i małe litery, cyfry i znak specjalny w postaci kropki.

Pamiętajmy jednak, że bardzo złą praktyką jest to, aby do każdego serwisu internetowego mieć ustawione to samo hasło, ponieważ w przypadku „wycieku” hasła przestępcy otrzymają dostęp do wszystkich naszych kont. Jak? Przestępcy będą próbowali zalogować się przy pomocy wykradzionych danych do popularnych serwisów. W końcu trafią na taki, w którym mamy założone konto, z hasłem, które już znają. Jeżeli koniecznie chcemy ćwiczyć naszą pamięć, możemy genero-

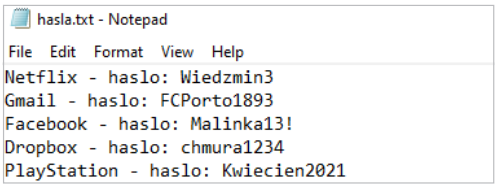
CIEKAWOSTKA

Niektóre oprogramowania służące do zarządzania hasłami, na przykład 1Password (https://1password.com), poinformują użytkownika, gdy ich dane znajdą się w internetowym „wycieku”, i poproszą go o zmianę haseł związanych z incydentem. Możesz też samodzielnie sprawdzić, czy twoje dane nie wyciekły, korzystając z darmowego serwisu Have I Been Pwned (https://haveibeenpwned.com/).

wać za pomocą zaproponowanej metody różne hasła do każdego serwisu internetowego. Możemy również wykorzystać do tego specjalny program nazywany „managerem haseł” (ang. *password manager*).

CO TO JEST MANAGER HASEŁ?

Manager haseł to oprogramowanie komputerowe, które pozwala generować silne (czyli długie, losowe i skomplikowane) hasła, a następnie zapisać je w pamięci komputera, telefonu lub nawet w chmurze. Pomyśl o nim, jak o cyfrowym sejfie, który będzie przechowywał ważne dla ciebie dane. W przeciwieństwie do haseł przechowywanych w formie zwykłego tekstu (ang. *plain text*, Ilustracja 1) hasła znajdujące się w managerze haseł są zaszyfrowane z wykorzystaniem silnych i sprawdzonych mechanizmów kryptograficznych i aby uzyskać do nich dostęp, musisz znać do nich hasło główne (Ilustracja 2).



Ilustracja 1. Przechowywanie haseł w zwykłym dokumencie tekstowym nie jest bezpieczne i nie jest zalecane. Prezentowane na ilustracji hasła nie są uważane za „silne”

Ilustracja 2. Hasła przechowywane w pliku managera haseł są zaszyfrowane. Bez znajomości głównego hasła dostępu będą wyglądały jak „krzaki”

Dlaczego warto korzystać z managera haseł? Z kilku powodów:

- Może utworzyć za ciebie unikatowe hasła do każdej witryny lub aplikacji.
- Przechowuje hasła bezpiecznie na twoim komputerze, telefonie lub w chmurze. Wszystkie są zaszyfrowane i zabezpieczone przed dostępem innej, niepowołanej osoby (Ilustracja 2).
- Potrafi integrować się z przeglądarką internetową, umożliwiając tym samym wpisywanie haseł z użyciem jednego, wygodnego przycisku lub skrótu klawiszowego.

KTÓRY MANAGER HASEŁ WYBRAĆ?

Wszystko zależy od tego, z jakich systemów operacyjnych korzystasz na co dzień na swoim komputerze (Windows/macOS/Linux) oraz na swoim urządzeniu mobilnym (iOS/Android). Na rynku istnieją między innymi takie rozwiązania jak 1Password, LastPass, Bitwarden czy KeePass. Niektóre z nich są płatne i funkcjonują w postaci stron internetowych przechowujących dane w chmurze, inne to programy do zainstalowania na własnym komputerze lub telefonie, zapisujące plik z hasłami na lokalnym urządzeniu.

W ramach ćwiczeń zainstalujemy i skonfigurujemy manager haseł KeePass na systemie Windows. Jest to darmowa aplikacja, którą każdy może zainstalować na swoim komputerze. Plik z hasłami przechowywany jest lokalnie na dysku użytkownika.

Wejdź na stronę https://keepass.info/, wybierz z menu po lewej stronie *Downloads* i pobierz najnowszą wersję oprogramowania (w momencie pisania artykułu była to wersja 2.47).

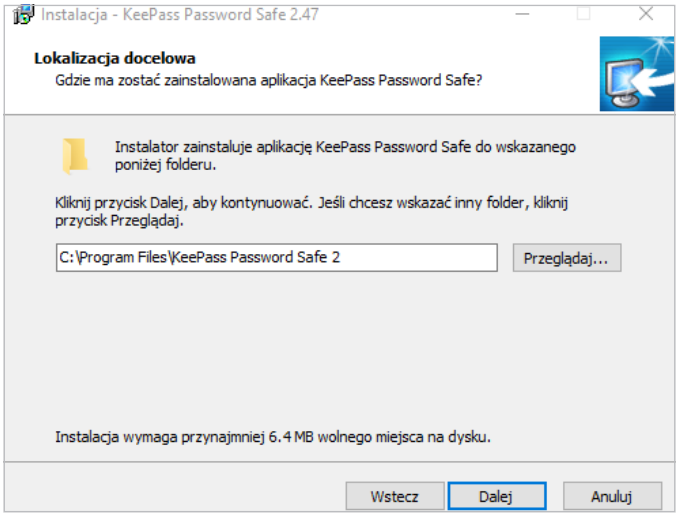
WARTO WIEDZIEĆ

Manager haseł może służyć również do przechowywania:

- zapasowych kodów utworzonych w trakcie dodawania aplikacji mobilnej w procesie dwuskładnikowego uwierzytelniania (2FA),
- kluczy licencyjnych do gier i programów,
- wrażliwych danych osobistych (numeru dowodu osobistego czy numeru PESEL),
- małych plików.

Ilustracja 3. Pobieranie managera haseł „KeePass” z oficjalnej strony keepass.info

Instalując oprogramowanie, będziesz musiał/a wybrać preferowany język oraz ścieżkę instalacyjną.

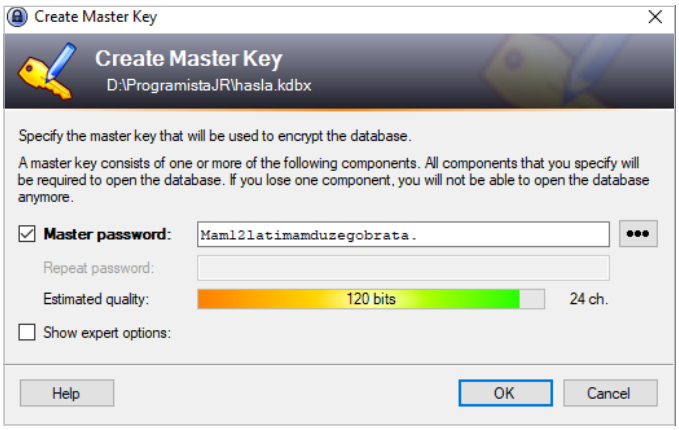


Ilustracja 4. Wybór ścieżki instalacyjnej „KeePass”

Zależnie od preferencji, w trakcie instalacji zaznacz opcję „Utwórz skrót na pulpicie”. Jeżeli nie jesteś doświadczonym użytkownikiem, pozostałe opcje pozostaw w domyślnej konfiguracji. Po zakończeniu instalacji uruchom aplikację KeePass.

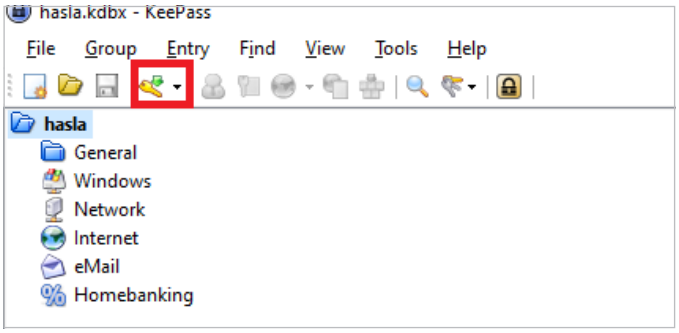
W lewym górnym rogu, z menu wyboru opcji *File* wybierz *New* (lub użyj skrótu klawiszowego Ctrl+n), by utworzyć pierwszą bazę haseł. Aplikacja poprosi o podanie nazwy i wybranie miejsca do przechowywania pliku o rozszerzeniu .kdbx (jest to format obsługiwany przez oprogramowanie KeePass). Kolejnym krokiem jest ustalenie hasła głównego do naszej bazy haseł, która będzie przechowywana w tym pliku. Ja posłużę się hasłem, które zaproponowałem na początku artykułu (Mam12latimamduzegobrata.), ale ty utwórz własne.

Uwaga! Jeżeli zapomnisz hasła do głównego pliku, nie będziesz mógł/mogła uzyskać dostępu do odszyfrowanej zawartości, dlatego dobrze przemyśl i zapamiętaj swój wybór.



Ilustracja 5. Ustawienie hasła głównego do bazy danych managera haseł

Nowe wpisy do bazy tworzymy przez naciśnięcie ikony klucza z zieloną strzałką (lub przez naciśnięcie skrótu Ctrl+i).

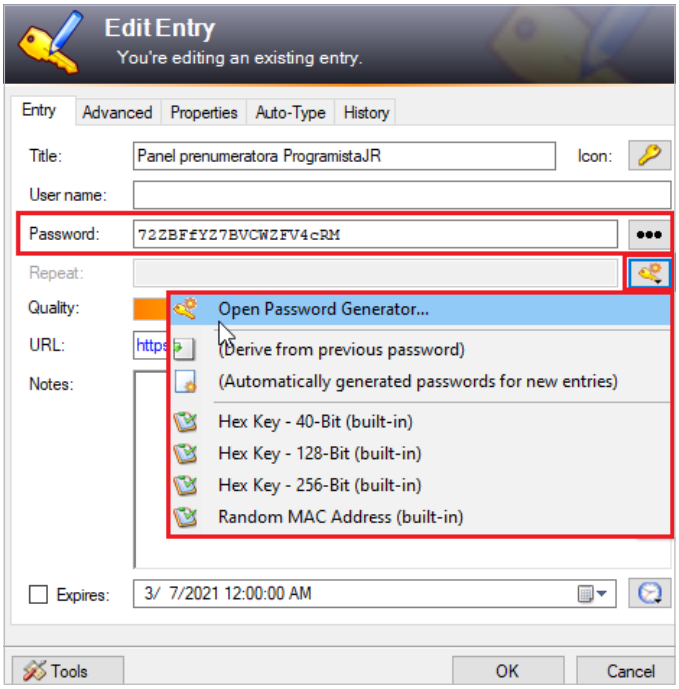


Ilustracja 6. Tworzenie pozycji w bazie managera haseł „KeePass”

Każda nowa pozycja ma losowo wygenerowane hasło, które można modyfikować ręcznie lub przy wykorzystaniu generatora haseł.

CIEKAWOSTKA

Zrób kopię zapasową pliku, który zawiera bazę haseł wykorzystywanych przez managera haseł. Zapisz ją na innym nośniku danych (na przykład na pendrivie). Wraz z upływem czasu do twojego managera haseł będą dochodziły kolejne pozycje, dlatego regularnie twórz kopie zapasowe bazy.



Ilustracja 7. Generowanie losowego hasła w managerze haseł „KeePass"

Wszystkie dodane rekordy dostępne są w głównym panelu. Dwukrotne kliknięcie na nazwę rekordu powoduje jego otwarcie. Dwukrotne kliknięcie w kolumnie hasła danego wiersza powoduje skopiowanie tego hasła do schowka - skopiowane hasło dostępne będzie w schowku jedynie przez 10 sekund.

Title	User Name	Password	URL	Notes
Panel prenumeratora Programis...		********	https://programistajr.pl/login/	
KeePass		********	https://keepass.info/	Notatki
Gmail		********	gmail.com	

Ilustracja 8. Lista utworzonych pozycji w managerze haseł „KeePass"

Naciśnięcie skrótu klawiszowego Ctrl+l powoduje ponowne zaszyfrowanie pliku z hasłami. Plik zostanie również zaszyfrowany, jeżeli zamkniemy aplikację. Po kolejnym otwarciu aplikacji KeePass wymagane jest podanie hasła głównego.

WARTO WIEDZIEĆ

Możesz dodatkowo zabezpieczyć dostęp do managera haseł, wymagając od użytkownika podania lokalizacji pliku z kluczem (ang. *key file*). Baza haseł zostanie odszyfrowana, tylko jeśli użytkownik poda prawidłowe hasło oraz wskaże lokalizację wcześniej ustalonego pliku z kluczem. Takie zabezpieczenie często stosowane jest przez osoby, które decydują się na tworzenie kopii zapasowej bazy danych managera haseł w chmurze (ang. *cloud*).

Zainstalowanie managera haseł i utworzenie pliku z bazą haseł to dopiero pierwszy krok, by poznać to rozbudowane narzędzie. KeePass pozwala między innymi na:

- tworzenie notatek do haseł,
- przechowywanie plików,
- integrację z przeglądarką internetową, umożliwiając tym samym automatyczne wpisywanie haseł do zapisanych stron z użyciem jednego, wygodnego przycisku lub skrótu klawiszowego.

Gorąco zachęcam do zapoznania się z wszystkimi funkcjami i wtyczkami aplikacji KeePass (https://keepass.info/help/base/firststeps.html).

Wiktor Szymański

Współzałożyciel serwisu bezpieczny.blog, sympatyk dzielenia się wiedzą, maniak planszówek, miłośnik książek i filmów szpiegowskich. Na co dzień zajmuje się dbaniem o bezpieczeństwo aplikacji webowych.

BEZPIECZNY.BLOG
KONTAKT@BEZPIECZNY.BLOG

ZAPAMIĘTAJ

- Ustaw silne, ale łatwe do zapamiętania hasło do managera haseł.
- Zrób kopię zapasową zaszyfrowanego pliku z hasłami.

ĆWICZ W DOMU

- Wygeneruj losowe hasła za pomocą managera haseł.
- Zacznij od mniej znaczących serwisów, żeby nabrać wprawy w korzystaniu z managera haseł.

Marcin Gromek

Uczymy się szyfrować pliki

Czasami zdarza się, że musimy wysłać wrażliwe dane mailem do kogoś z rodziny czy szkoły. Może to być świadectwo ukończenia szkoły, skan legitymacji szkolnej czy formularz z naszymi danymi personalnymi. Niekiedy zachodzi potrzeba, że takie dane musimy przenieść między komputerami na pendrivie. Jak zrobić to bezpiecznie, czyli w taki sposób, aby niepowołany „znalazca" nie mógł odczytać naszych danych?

12+

DOWIESZ SIĘ

- Jak zaszyfrować pliki programem 7-Zip.
- Jak odszyfrować pliki programem 7-Zip.

POTRZEBNA WIEDZA

- Jak pobierać i instalować aplikacje na komputerze z systemem Windows.

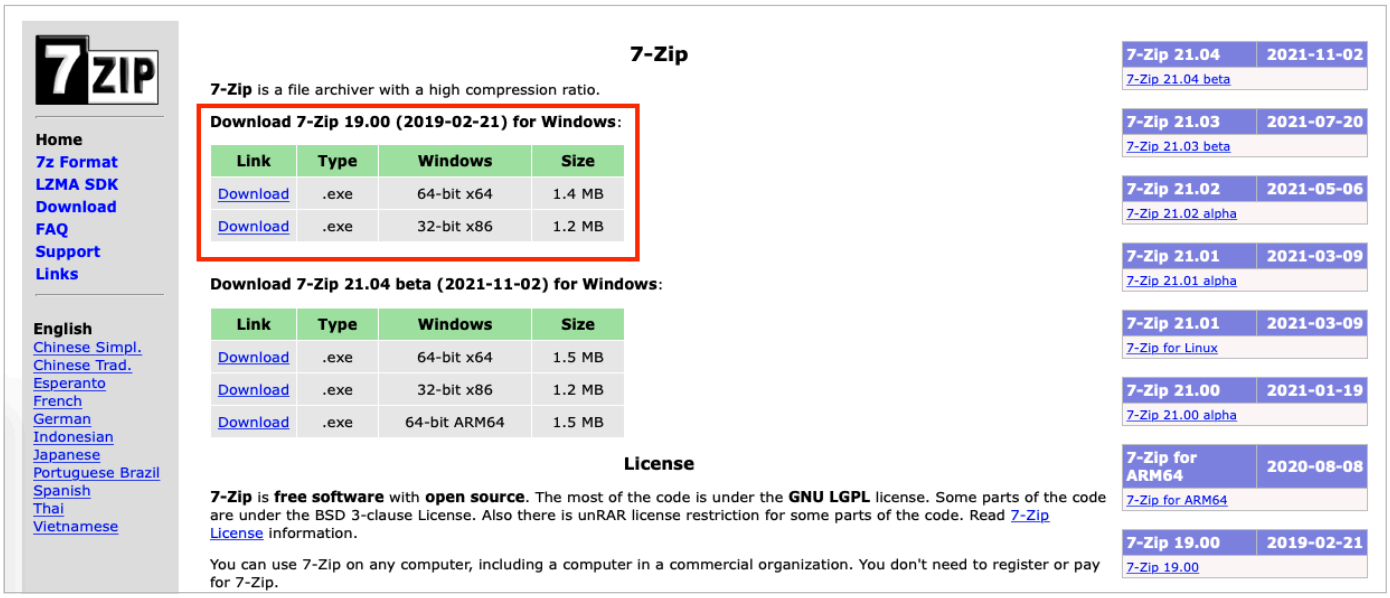
Dorośli często wysyłają drogą mailową takie swoje dane, jak:

- imię i nazwisko,
- nazwisko panieńskie matki,
- PESEL,
- numer i seria dowodu osobistego,
- skany różnych dokumentów.

Czasem urzędy czy prywatne firmy (na przykład ubezpieczeniowe) wymagają wysłania takich danych, aby wykonać określoną usługę. Wysyłając te dane w formie niezaszyfrowanej, narażamy się na możliwość ich ujawnienia w przypadku wycieku danych czy włamania na serwer pocztowy u odbiorcy korespondencji oraz u nas samych. Można też założyć, że te dane zostaną umyślnie lub przypadkiem zachowane na skrzynce odbiorczej adresata zamiast być skasowane niezwłocznie po przeniesieniu ich do wewnętrznych systemów urzędu czy firmy. Nie wspominając o tym, że zostaną w naszej skrzynce nadawczej. Takie dane mogą posłużyć przestępcy do podszycia się pod nas, na przykład występując o kredyt w banku.

Znacznie bezpieczniej jest przesłać zaszyfrowany plik z danymi, a hasło przekazać innym kanałem, czyli w inny sposób. Na przykład jeśli plik wysyłamy mailem, to hasło możemy przesłać SMS-em. W ten sposób, nawet jeśli nastąpi wyciek z serwera pocztowego adresata lub nadawcy, zawartość naszego pliku jest bezpieczna. Szyfrowanie może się także przydać, gdy przechowujemy dane na nośnikach wymiennych, jak na przykład pendrive. W przypadku zgubienia nośnika dane pozostaną bezpieczne.

Bezpieczeństwo danych zależy oczywiście od tego, jak mocnego hasła użyjemy. Polecam korzystanie z jak najdłuższych haseł, np. ponad 20 znaków. To właśnie długość hasła jest ważniejsza od jego poziomu skomplikowania. Oczywiście same małe litery nie wystarczą, więc zawsze warto dorzucić kilka cyfr i znaków specjalnych, takich jak $, & czy %. Stosowanie imion, nazwisk i dat urodzenia nie jest dobrym pomysłem, bo łatwo je odgadnąć. Hasło powinno składać się z losowych słów. Przykładem silnego hasła jest „Mam12latimamduzegobrata." zaproponowane w artykule Wiktora Szymańskiego pod tytułem „Używamy managera haseł".



Ilustracja 1. Oficjalna strona programu 7-Zip

CZYM SZYFROWAĆ

Jest wiele programów, które mogą nam pomóc w szyfrowaniu plików na każdym z wiodących systemów operacyjnych używanych na komputerach. Jednocześnie przestrzegam przed używaniem stron internetowych obiecujących odesłanie nam zaszyfrowanego pliku, po załadowaniu go na stronie, bez konieczności instalacji oprogramowania na komputerze. W ten sposób przesyłamy przez Internet nasze dane bez ochrony i bez wiedzy, do kogo mogą one trafić.

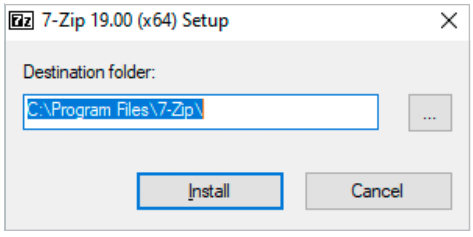
Na potrzeby tego artykułu skupimy się na programie (a właściwie zbiorze programów) 7-Zip dostępnym na system Windows. Jest to popularny, darmowy program o otwartym kodzie, przeznaczony do kompresji, dekompresji i szyfrowania danych. Jego główną funkcją jest kompresowanie, czyli pakowanie jednego lub więcej plików do jednego pliku (tak zwanego archiwum), który ma zazwyczaj mniejszy rozmiar niż suma wejściowych plików. Z 7-Zipa można korzystać do celów prywatnych i komercyjnych bez ponoszenia kosztów.

Aby zainstalować program 7-Zip, wejdź na stronę https://www.7-zip.org (Ilustracja 1). W tabeli z nagłówkiem w kolorze zielonym jest link do ściągnięcia aktualnej wersji (w momencie pisania tego artykułu jest to wersja 19.00). Możesz wybrać wersję 64-bit lub 32-bit, choć dla większości użytkowników odpowiednia będzie wersja 64-bit. Możesz też ściągnąć wersje 21.04 beta, ale pamiętaj, że wersja beta jest wersją testową, a więc może zawierać błędy. Niezależnie od wersji instalator nie zajmuje więcej niż 1,5 MB.

WARTO WIEDZIEĆ

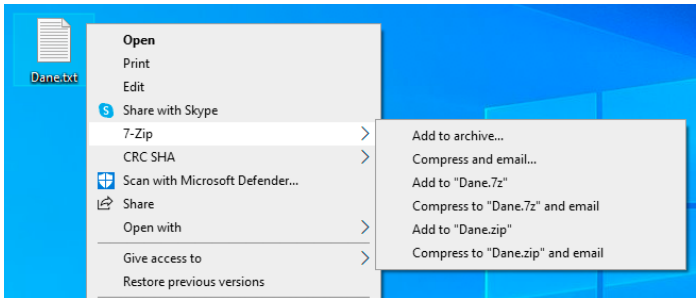
Szyfrowanie to zamiana tekstu jawnego, czyli danych, które chcemy zaszyfrować (na przykład plik PDF zawierający skan dokumentu) na szyfrogram, czyli zabezpieczoną kluczem (wygenerowanym z hasła) postać tych danych, przy pomocy algorytmu kryptograficznego, czyli specjalnej funkcji matematycznej. Takie algorytmy dzielimy na symetryczne i asymetryczne. Algorytm symetryczny (na przykład AES-256) to taki, który korzysta z jednego klucza zarówno do szyfrowania, jak i odszyfrowywania. Algorytm asymetryczny wymaga osobnych kluczy do każdego z tych działań.

Instalacja tego programu jest bardzo prosta – po uruchomieniu instalatora wystarczy wybrać ścieżkę instalacji programu (Ilustracja 2) i kliknąć Install.



Ilustracja 2. Wybór ścieżki instalacji programu 7-Zip

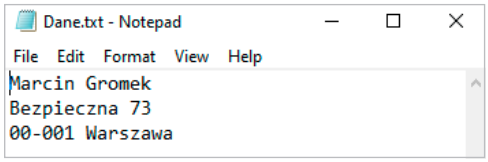
Po zainstalowaniu program tworzy nową, rozwijaną pozycję o nazwie 7-Zip w menu kontekstowym, które można wywołać, klikając prawym przyciskiem myszy na plikach lub katalogach (Ilustracja 3). Poza najprostszą pozycją *Add to archive* (z ang. dodaj do archiwum), która z wybranego pliku utworzy skompresowanie archiwum, dostępne są inne ciekawe opcje. Opcja *Compress and email* pozwala na skompresowanie plików i następnie umieszczenie wynikowego archiwum jako załącznik w programie pocztowym skonfigurowanym w naszym systemie jako domyślny. Funkcja *Add to "Dane.7z"* pozwala na dodanie plików do archiwum o nazwie Dane.7z, a jeśli to archiwum już istnieje, to dodanie do niego pliku, jeśli archiwum nie zawiera pliku o takiej nazwie. Nazwa Dane.7z jest zgodna z nazwą pliku, na który kliknęliśmy.



Ilustracja 3. Menu kontekstowe dodane po instalacji dla nieskompresowanych plików

JAK SZYFROWAĆ

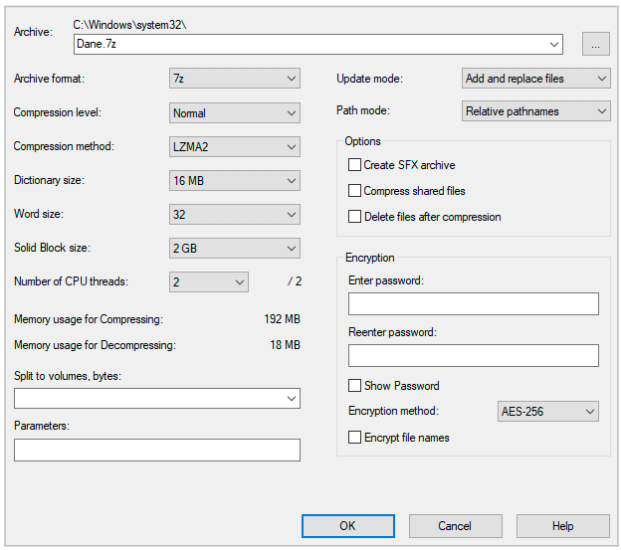
Na potrzeby tego artykułu stworzyłem plik tekstowy z pewnymi danymi (Ilustracja 4). Możesz wybrać plik lub pliki o dowolnym rozszerzeniu i rozmiarze, ale im mniejszy i prostszy, tym szybciej zostanie zaszyfrowany.



Ilustracja 4. Przykładowy plik tekstowy „Dane.txt"

W tym przykładzie użyjemy pozycji *Add to archive* z menu kontekstowego, która z wybranego pliku pozwoli nam stworzyć skompresowane i zaszyfrowane archiwum. Po wybraniu tej pozycji naszym oczom ukaże się okno programu (Ilustracja 5). Przyjrzyjmy się dostępnym opcjom, które są istotne z punktu widzenia naszego celu.

- *Archive* – pokazuje ścieżkę do archiwum, czyli zaszyfrowanego pliku. Warto zmienić ją z domyślnej na coś bardziej dostępnego dla użytkownika (na przykład folder Dokumenty czy Pulpit) poprzez kliknięcie przycisku z wielokropkiem po lewej stronie od formularza. Domyślnie nazwa wynikowego pliku jest taka sama jak wybranego pliku lub folderu.
- *Archive format* – rozszerzenie wynikowego pliku archiwum. Domyślnie jest to .7z, ale można wybrać inne. Trzeba jednak pamiętać, że jedynie formaty .7z oraz .zip wspierają szyfrowanie.
- *Enter password* – tu podajemy hasło, którym będzie zaszyfrowany plik.
- *Reenter password* – tu ponownie podajemy hasło, w celu weryfikacji i uniknięcia ustawienia błędnego hasła.
- *Show password* – możemy zaznaczyć tę opcję, jeśli chcemy widzieć znaki wpisywane w polu *Enter password*. Jeśli wybierzemy tę opcję, pole *Reenter password* zniknie.
- *Encryption method* – wybór algorytmu, który zostanie użyty do szyfrowania pliku.
- *Encrypt file names* – zaszyfrowanie nazw plików.



Ilustracja 5. Okno programu pokazujące dostępne opcje

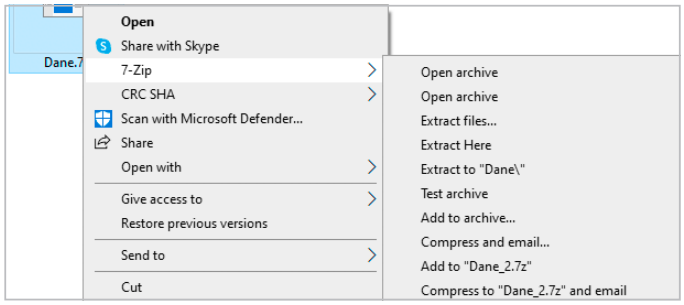
Po kliknięciu przycisku OK wybrany plik zostanie utworzony we wskazanej ścieżce – w tym przykładzie w folderze Dokumenty. Plik jest gotowy do wysłania pocztą e-mail lub przekopiowania na pendrive.

CIEKAWOSTKA

Algorytm AES-256 (ang. Advanced Encryption Standard), który jest używany przez 7-Zip, został przyjęty w 2001 roku jako standard przez amerykańską agencję NIST w miejsce algorytmu DES (ang. Data Encryption Standard). Został on również przyjęty przez amerykańską agencję bezpieczeństwa NSA do ochrony ściśle tajnych informacji. 256 to liczba bitów, z której składa się (wygenerowany z hasła) klucz. W praktyce im większa długość klucza, tym dłużej trwa proces szyfrowania, ale za to szyfrowanie jest trudniejsze do złamania.

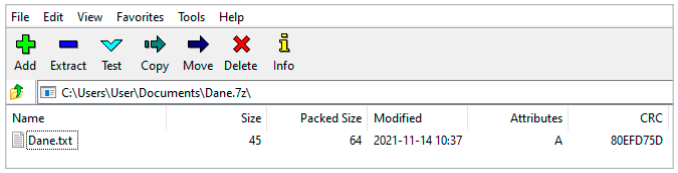
JAK ODSZYFROWAĆ

Teraz skupimy się na rozpakowaniu i odszyfrowaniu archiwum. Jeśli otrzymaliśmy od kogoś zaszyfrowane archiwum, to klikamy na niego prawym przyciskiem myszy i przechodzimy do pozycji *7-Zip*. Pokaże się menu kontekstowe z pozycjami przeznaczonymi dla plików archiwów (Ilustracja 6).



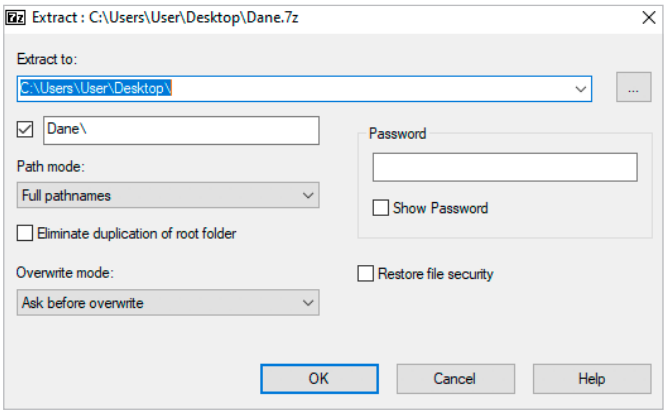
Ilustracja 6. Menu kontekstowe dla skompresowanych plików

Poza pozycjami, które znamy już z Ilustracji 3 (bo gotowy plik archiwum można ponownie skompresować i zaszyfrować), mamy dostępne także inne pozycje, jak *Open archive* czy kilka funkcji *Extract*. Pozycja *Open archive* spowoduje otwarcie zawartości archiwum w przeglądarce plików *7-Zip File Manager* (Ilustracja 7). Dopiero po kliknięciu na widoczną nazwę pliku pokaże się okno dialogowe z prośbą o wprowadzenie hasła.



Ilustracja 7. Okno programu 7-Zip z listą plików w archiwum

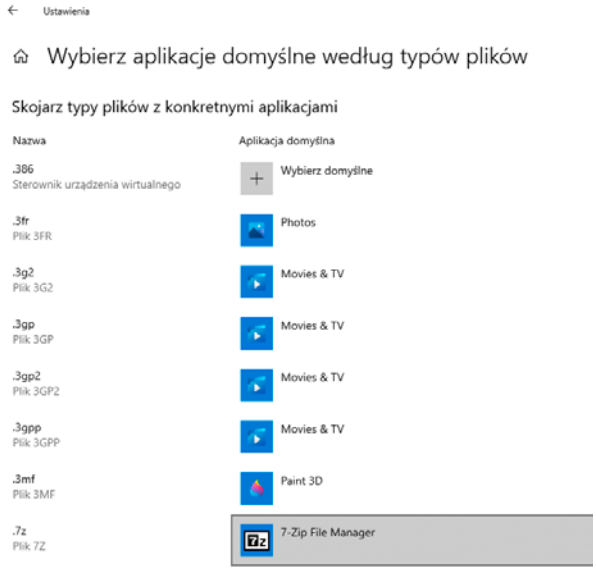
Wybranie pozycji *Extract files* spowoduje otwarcie okna dialogowego (Ilustracja 9) między innymi z prośbą o wskazanie ścieżki do folderu, do którego użytkownik chce wypakować pliki, a także miejscem na wprowadzenie hasła (jeśli go nie podamy, program zapyta nas o to później).



Ilustracja 9. Okno dialogowe po wybraniu funkcji „Extract files”

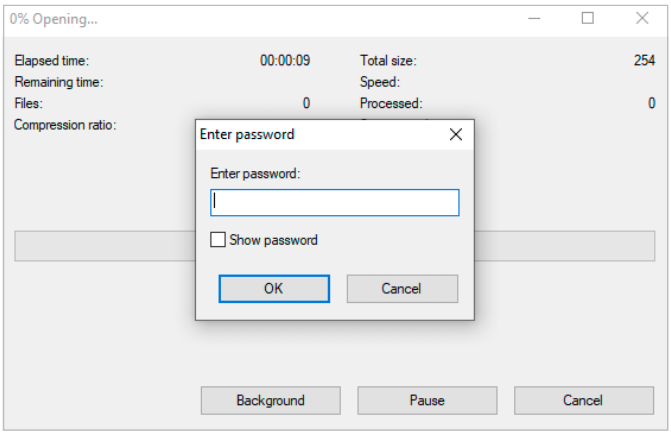
WARTO WIEDZIEĆ

Jeśli w ustawieniach systemu Windows (Ustawienia > Aplikacje > Aplikacje domyślne > Wybierz aplikacje domyślne według typów plików) zaznaczymy, żeby pliki z rozszerzeniami .7z były domyślnie obsługiwane przez program 7-Zip File Manager, to będziemy mogli łatwiej odpakowywać i rozszyfrować archiwa – poprzez dwukrotne kliknięcie lewym przyciskiem myszy na spakowany plik.



Ilustracja 8. Lista rozszerzeń z domyślnymi aplikacjami do wyboru

Wybranie pozycji *Extract here* lub *Extract to „Dane\”* spowoduje odpowiednio rozpakowanie danych do tego samego folderu, w którym znajduje się plik archiwum, lub utworzenie folderu o nazwie takiej samej jak plik archiwum i umieszczenie w nim rozpakowywanych plików. Obie akcje zostaną poprzedzone prośbą o wprowadzenie hasła (Ilustracja 10).



Ilustracja 10. Okno dialogowe z prośbą o wprowadzenie hasła

SZYFROWANIE NAZW PLIKÓW

Opcja *Encrypt file names*, widoczna w oknie programu 7-Zip podczas tworzenia archiwum (Ilustracja 5), jest często pomijana przez użytkowników, a moim zdaniem jest bardzo przydatna. Wybranie jej spowoduje, że zaszyfrowana zostaje nie tylko zawartość plików, ale także ich nazwy. Jeśli więc mamy pliki, których nazwy wskazują na zawartość (na przykład Jan_Kowalski_skan_dowodu.pdf), warto skorzystać z tej opcji. W ten sposób potencjalny „znalazca” pliku nie będzie miał podpowiedzi o tym, co może znajdować się w środku archiwum. W praktyce wygląda to tak:

a. Jeśli opcja *Encrypt file names* została wybrana – po kliknięciu prawym przyciskiem na plik archiwum Dane.7z i wybraniu z menu kontekstowego 7-Zip pozycji *Open archive* od razu pokazuje się okno dialogowe z prośbą o wprowadzenie hasła (Ilustracja 10) zanim pokazane zostaną nazwy plików zawartych w archiwum.

b. Jeśli opcja *Encrypt file names* nie została wybrana – po kliknięciu prawym przyciskiem na plik archiwum Dane.7z i wybraniu z menu kontekstowego 7-Zip pozycji *Open archive* pokazuje się okno z listą plików w archiwum (Ilustracja 7). Dopiero po kliknięciu na któryś z plików pokazuje się okno dialogowe z prośbą o wprowadzenie hasła (Ilustracja 10).

Marcin Gromek

Ekspert ds. bezpieczeństwa IT. Uwielbia słuchać podcastów i pić dobrą kawę. Pisze i nagrywa dla serwisu bezpieczny.blog.

KONTAKT@BEZPIECZNY.BLOG
HTTPS://BEZPIECZNY.BLOG

ZAPAMIĘTAJ

- Szyfrowanie danych pozwala ograniczyć konsekwencje wycieku przekazywanych przez nas danych na przykład drogą mailową.
- Używaj funkcji „Encrypt file names”, która powoduje szyfrowanie nie tylko zawartości archiwum, ale także nazw plików, które zawiera.
- Szyfrowanie plików przydaje się również przy przekazywaniu danych za pomocą nośników wymiennych, takich jak pendrive.

ĆWICZ W DOMU

- Spróbuj nauczyć inne osoby, jak pakować oraz szyfrować dane wrażliwe przed wysłaniem ich mailem.
- Zapoznaj się z innymi funkcjami kompresowania i szyfrowania programu 7-Zip.

Wiktor Szymański

Kopia bezpieczeństwa

„I need backup!" (z ang. potrzebuję wsparcia) to popularny zwrot, który możemy często usłyszeć z ust bohaterów filmów akcji lub gier komputerowych, wypowiadany najczęściej w sytuacjach kryzysowych. Słowo „backup" w terminologii komputerowej oznacza kopię zapasową, której posiadanie może uratować użytkownika przez nieprzespanymi nocami i potwornym bólem głowy.

10+

DOWIESZ SIĘ

- Czym jest kopia bezpieczeństwa i dlaczego warto ją wykonywać.

POTRZEBNA WIEDZA

- Wiedza o tym, jakie dane są dla nas ważne.

Kopia zapasowa (zwana również kopią bezpieczeństwa) to zapasowa wersja danych, która ma służyć użytkownikowi do odtworzenia oryginalnego zbioru danych w wypadku ich utraty lub uszkodzenia. Podobno ludzie dzielą się na tych, którzy robią kopie zapasowe, i na tych, którzy będą je robili[1]. Utrata ważnych danych, połączona ze świadomością, że można było się na taką sytuację przygotować (poprzez wykonywanie kopii zapasowej), sprawia, że wiele osób podejmuje decyzje o rozpoczęciu wykonywania cyklicznych backupów.

Często wyobrażamy sobie, że takie rzeczy, jak kradzież, uszkodzenie laptopa czy utopienie telefonu w jeziorze, to historie, które przydarzają się innym osobom, ale na pewno nie nam. Rzeczywistość bywa jednak kapryśna. Pod koniec 2021 roku w moim laptopie padł dysk. Po przeżyciu chwili grozy związanej z obawą o moje zdjęcia i dokument szybko nadeszło uczucie ulgi. Byłem przygotowany na taką sytuację, ponieważ kopie bezpieczeństwa ważnych dla mnie plików wykonuję od ponad 10 lat. Muszę uczciwie powiedzieć, że samo wykonywanie kopii zapasowej nie jest zajęciem szczególnie interesującym, ciężko jednak jest mi znaleźć uczucie bardziej satysfakcjonujące niż to związane z odtworzeniem danych z kopii zapasowej po utracie lub uszkodzeniu oryginalnego nośnika.

1. Na pewno niejednokrotnie przeczytasz lub usłyszysz ten zwrot w swoim życiu.

DANE DANYM NIERÓWNE

Wykonanie kopii zapasowej powinno zostać poprzedzone analizą tego, jakie dane są dla nas ważne. Dla jednych będą to zdjęcia i filmy, inni za wszelką cenę będą chcieli chronić swoje rysunki czy opowiadania, jeszcze inni skupią się na swoich kontaktach, rozmowach z komunikatorów czy stworzonych liniach kodu. Żeby móc zidentyfikować ważne dla nas dane, zachęcam do przeprowadzenia prostego ćwiczenia: Wyobraźmy sobie, że w tym momencie na zawsze tracimy dostęp do swojego telefonu i komputera. Jakie informacje czy dokumenty na nich zawarte przepadłyby nieodwracalnie? Których byłoby nam najbardziej szkoda? Usiądź i wypisz na kartce swoje przemyślenia. Właśnie wykonałeś/aś pierwszy krok do utworzenia kopii zapasowej – przeprowadziłeś/aś analizę danych, dla których chcesz wykonać backup.

GDZIE PRZECHOWYWAĆ KOPIĘ BEZPIECZEŃSTWA?

Istnieje wiele miejsc, w których możemy przechowywać kopię bezpieczeństwa. Myślę, że miejsca te możemy przyporządkować do jednej z dwóch kategorii:

- Pamięć zewnętrzna (na przykład: pendrive, dysk zewnętrzny, dysk sieciowy (ang. NAS – *Network-attached storage*)).
- Serwisy zewnętrzne, usługi chmurowe.

Dobrą praktyką jest przechowywanie kopii bezpieczeństwa w dwóch różnych miejscach, na wypadek utraty dostępu do jednego z nich.

Załóżmy, że w przeprowadzonym przeze mnie przed chwilą ćwiczeniu jako ważne dla mnie dane wskazałem:

- zdjęcia,
- skany dokumentów,
- bazę z managera haseł KeePass[2],
- napisany przeze mnie kod.

Stosując się do dobrych praktyk, chciałbym, żeby kopia zapasowa ważnych dla mnie danych przechowywana były w dwóch niezależnych miejscach (dysk zewnętrzny oraz chmura) i żeby dla chociaż jednego z tych miejsc kopia wykonywała się w miarę automatycznie. Dobrałem do moich danych następujące miejsca, w których przechowywał będę ich kopie zapasowe:

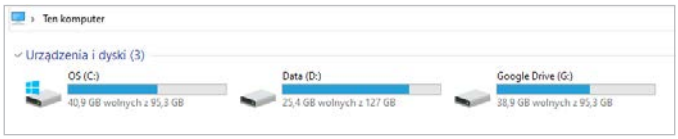
- zdjęcia – Google Photos (photos.google.com),
- skany dokumentów – Google Drive (drive.google.com),
- bazę z managera haseł KeePass – Google Drive,
- kod – repozytorium kodu GitHub (github.com).

Jestem użytkownikiem komputera z systemem Windows i telefonu z systemem Android, mój e-mail znajduje się w serwisie Gmail (gmail.com). Biorąc pod uwagę te czynniki, postanowiłem większość moich danych przechowywać w serwisach oferowanych przez firmę Google, która zapewnia oprogramowanie dla swoich usług (Google Photos oraz Google Drive) działające zarówno na moim telefonie, jak i komputerze, co ułatwia mi synchronizację moich danych. Kod moich projektów przechowuję w serwisie GitHub, który jest największą platformą do przechowywania kodu. Jednocześnie raz w miesiącu ręcznie przerzucam wszystkie ważne dla mnie dane na dysk zewnętrzny.

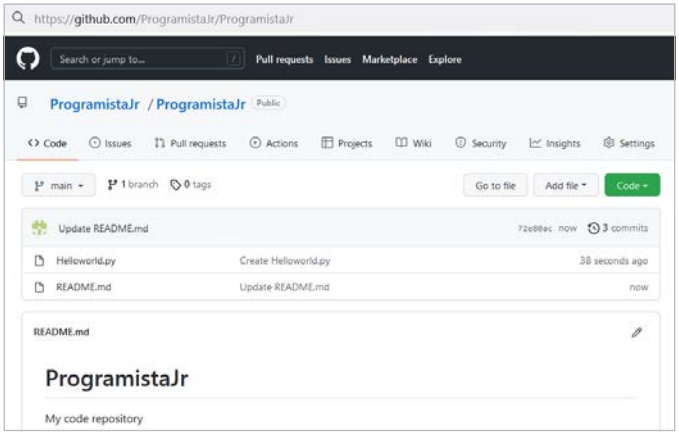
Oczywiście powyższe propozycje to tylko przykład. Wychodzę z założenia, że niezależnie od tego, z jakich serwisów i programów korzystasz, dopóki wykonujesz kopię bezpieczeństwa ważnych dla siebie danych i jesteś w stanie je odtworzyć w przypadku utraty oryginalnego nośnika, to twój sposób jest dobry. Reszta to rzecz gustu i technikalia.

WARTO WIEDZIEĆ

Często w trakcie dyskusji o kopiach zapasowych czy redundancji danych usłyszeć można sformułowanie **RAID** (ang. *Redundant Array of Independent Disks*). Jest to sposób połączenia dwóch lub większej ilości dysków twardych w jedną macierz (widoczną jako jeden dysk). Dane przechowywane na macierzy RAID zapisywane są jednocześnie na kilku dyskach twardych, dzięki czemu w przypadku awarii jednego z nich dostępność danych nie ulega zmianie. Macierze RAID są powszechnie stosowane w rozwiązaniach serwerowych, dzięki czemu uzyskiwana jest odporność na awarie oraz zwiększenie prędkości transmisji w porównaniu z pojedynczym dyskiem.



Ilustracja 1. Podpięty dysk Google Drive w komputerze może służyć jako miejsce przechowywania kopii bezpieczeństwa. Wybrane foldery znajdujące się na komputerze mogą być automatycznie synchronizowane z chmurą



Ilustracja 2. Kopię swojego kodu można przechowywać za darmo w repozytorium kodu GitHub

2. O wykorzystaniu managera haseł przeczytasz w artykule „Używamy managera haseł".

BEZPIECZEŃSTWO KOPII DANYCH

Wykonując kopię zapasową, należy bezwzględnie zadbać o jej bezpieczeństwo poprzez:

- zabezpieczenie (fizycznego lub cyfrowego) dostępu do nośnika, na którym przechowywana jest zapasowa kopia danych
- szyfrowanie plików z wrażliwymi danymi lub całego nośnika.

W przypadku przechowywania danych w chmurze (na przykład na dysku Google Drive) warto pamiętać, że dane przechowywane na wirtualnym dysku zabezpieczone są w tym samym stopniu, w jakim zabezpieczone jest nasze konto, którym logujemy się do usługi. Przydatne rady dotyczące zabezpieczenia poczty gmail (oraz dysku Google Drive) przedstawiono w artykule „Jak zabezpieczyć pocztę gmail?".

Jeżeli w skład naszej kopii bezpieczeństwa wchodzą dane, które uważamy za wrażliwe, powinniśmy rozważyć ich szyfrowanie. W przypadku utraty naszej kopii bezpieczeństwa osoba, która wejdzie w jej posiadanie, nie będzie mogła ich odczytać. O tym, jak szyfrować pliki z wykorzystaniem programu 7-Zip, przeczytacie w artykule Marcina Gromka „Uczymy się szyfrować pliki".

Jeżeli jeszcze nie czytaliście wyżej wymienionych artykułów, to serdecznie zapraszam do nadrobienia zaległości.

WEHIKUŁ CZASU

Zdarza się, że największy zysk z wykonanych kopii danych osiągamy po latach, nie dzięki potrzebie ich odtworzenia w krytycznym momencie, lecz dzięki wartości sentymentalnej, jaką przez lata dla nas nabierają. Stare zdjęcia, utwory muzyczne, zapisy w wirtualnym pamiętniku znalezione po wielu latach zyskują niesamowitą moc i potrafią być wielkim źródłem szczęścia. Chociażby po to warto wykonać od czasu do czasu kopię zapasową.

CIEKAWOSTKA

Niestety nie wszyscy dorośli wykonują kopie zapasowe danych, które są dla nich ważne.

Zapytaj rodziców lub opiekunów, w jaki sposób wykonują kopie bezpieczeństwa swoich plików. Jakie pliki są dla nich ważne? Czy 10-15 lat temu wykonywali kopie bezpieczeństwa? Jak zmieniły się nośniki danych, na których trzymali swój backup?

Wiktor Szymański

Współzałożyciel serwisu bezpieczny.blog, fan LEGO, sympatyk dzielenia się wiedzą, maniak planszówek, miłośnik książek i filmów szpiegowskich. Na co dzień zajmuje się dbaniem o bezpieczeństwo aplikacji webowych.

HTTPS://BEZPIECZNY.BLOG
KONTAKT@BEZPIECZNY.BLOG

ZAPAMIĘTAJ

- Ludzie dzielą się na tych, którzy robią kopie zapasowe, i na tych, którzy będą je robili – lepiej należeć do tej pierwszej grupy.
- Wykonanie kopii zapasowej powinno zostać poprzedzone analizą tego, jakie dane są dla nas ważne.
- Kopie zapasowe oraz miejsca, w których je przechowujemy, powinny być odpowiednio zabezpieczone.

ĆWICZ W DOMU

- Zapytaj rodziców lub opiekunów, w jaki sposób wykonują kopie bezpieczeństwa swoich plików.
- Zastanów się, jakie dane przechowywane na twoim komputerze lub telefonie są dla ciebie ważne.
- Wykonaj pierwszą kopię bezpieczeństwa swoich danych.

BLENDER

Modelowanie postaci

BLENDER

Modelowanie konia

szkolenia wideo z zakresu grafiki 3d

www.keylight.com.pl

Druk 3d z ZBrushem

ZBRUSH

Modelowanie w ZBrushu

ZBRUSH

Marcin Gromek

O czym pamiętać, konfigurując router

Dzisiejsze routery domowe to skomplikowane urządzenia. Mają wiele różnych funkcji, które często chowają się za zagadkowymi akronimami. Postaram się wyjaśnić działanie najpopularniejszych funkcji oraz doradzić, jak skonfigurować router, aby nasza domowa sieć stała się bezpieczniejsza.

10+

DOWIESZ SIĘ

- Jak poprawić bezpieczeństwo domowej sieci.
- Jakie funkcje zazwyczaj mają domowe routery.

POTRZEBNA WIEDZA

- Podstawowa wiedza z zakresu sieci komputerowych.
- Możliwość konfigurowania routera.

CZEMU KUPOWAĆ DODATKOWE URZĄDZENIE?

Operator Internetu (jak dostawca telewizji kablowej, operator komórkowy czy operator sieci światłowodowej) zazwyczaj przekazuje nam urządzenie (często nazywane modemem), które pozwala nam połączyć się z Internetem zarówno przez Wi-Fi, jak i przy użyciu kabla sieciowego. Może ono jednak mieć kilka wad:

- brak pełnej kontroli – zdarza się, że operator może sterować niektórymi funkcjami;
- brak aktualizacji, w tym poprawek bezpieczeństwa – szybko przestaje być aktualizowane przez producenta;
- brak niektórych funkcji – ma jedynie podstawowe funkcje;
- domyślna konfiguracja może nie być bezpieczna – takie urządzenie ma działać od razu po podłączeniu, więc ma włączone nadmiarowe usługi.

Między innymi z tych względów warto zaopatrzyć się w osobny router. Na modemie od operatora można wtedy wyłączyć wszystkie usługi, które nie są nam bezpośrednio potrzebne do korzystania z Internetu lub innych usług, które wykupiliśmy (na przykład telewizji, telefonu stacjonarnego). Dodatkową korzyścią z takiej konfiguracji jest ukrycie naszego routera za urządzeniem od operatora, co utrudni ataki z Internetu. Należy pamiętać, że nie wszystkie opisane w artykule funkcje są dostępne na każdym routerze.

KONFIGURACJA PO KABLU

Przy pierwszym uruchomieniu routera wiele usług jest już uruchomionych, aby pozwolić użytkownikowi na szybkie rozpoczęcie korzystania z urządzenia. Może też być włączone Wi-Fi. Jeśli kupiliśmy sprzęt, który ma powszechnie znane domyślne hasło do sieci bezprzewodowej, to ktoś może się do niego podłączyć bez naszej zgody. Jeśli to możliwe, dobrze jest wykręcić anteny routera przed uruchomieniem i podłączyć się do routera przy użyciu kabla sieciowego. Przyspieszy to też konfigurację, jeśli urządzenie resetuje interfejsy bezprzewodowe przy zmianie konfiguracji – nie będziemy musieli czekać na ponowne podłączenie się do sieci Wi-Fi.

WARTO WIEDZIEĆ

Polskie prawo nie nakazuje wprost właścicielom sieci Wi-Fi zabezpieczenia jej. Jeśli jednak ktoś dostanie się do naszej sieci i przeprowadzi atak lub dokona przestępstwa, to policja zapuka w pierwszej kolejności do naszych drzwi.

DANE KONTA ADMINISTRACYJNEGO

Dobrym pierwszym krokiem podczas konfigurowania routera jest zmiana nazwy użytkownika administracyjnego i jego hasła. Każdy nowoczesny router ma takiego użytkownika, który pozwala na dostęp do panelu administracyjnego (często dostępnego pod adresem 192.168.0.1 lub 192.168.1.1). Domyślne dane do logowania mogą być powszechnie znane, na przykład zapisane w instrukcji obsługi dostępnej w Internecie. Rzadziej są one unikalne i nadrukowane na etykiecie urządzenia. Niegdyś popularnym zestawem danych do logowania był login: admin i hasło: admin. Używanie prostych, standardowych loginów i haseł ma na celu ułatwienie użytkownikowi życia, ale stanowi zagrożenie dla bezpieczeństwa naszej sieci. Zależnie od urządzenia może się zdarzyć, że nazwa użytkownika nie jest możliwa do zmiany. Jako nowe hasło należy wybrać silne, unikalne i niesłownikowe hasło (podobnie jak na przykład do serwisów internetowych). Najlepiej takie hasło przechowywać w managerze haseł. Więcej o hasłach możesz przeczytać w artykule Wiktora Szymańskiego „Używamy managera haseł", opublikowanego w numerze 2/2021 (10).

NAZWA I HASŁO DO SIECI BEZPRZEWODOWEJ

Domyślna nazwa sieci bezprzewodowej może wskazywać na urządzenie, z którego korzystamy, bo na przykład zawiera jego model lub numer seryjny. Możliwe jest nawet, że może ona posłużyć do odgadnięcia hasła do sieci, jak miało to miejsce w przypadku modemów dostarczanych przez jednego z operatorów sieci kablowych w Polsce. Jeśli chodzi o hasło, to oczywiście powinno być ono silne, unikalne i niesłownikowe, ale pamiętaj, że będzie je trzeba wprowadzić ręcznie na wszystkich urządzeniach. Lepiej, żeby takie hasło składało się z wielu prawdziwych słów przeplatanych znakami specjalnymi i liczbami, niż żeby było losowym ciągiem znaków.

FIREWALL

Routery często są wyposażone w zaporę ogniową (ang. *firewall*), czyli prosty program, który nie wpuszcza pakietów pochodzących z serwerów w Internecie, do których wcześniej nie nawiązano połączenia z wewnątrz sieci. Jeśli wpiszesz w przeglądarce adres https://bezpieczny.blog, komputer inicjuje ruch do serwera serwisu bezpieczny.blog. W ruchu tym pośredniczy router. Ruch powrotny z serwera, zawierający treść bloga, zostanie przepuszczony przez firewall, ponieważ ten wcześniej widział ruch wychodzący. W ten sposób chronimy sieć domową przed częścią ataków z zewnątrz. Mogą istnieć predefiniowane tryby pracy *firewalla*, na przykład słaby, średni i silny, ale zdarza się, że można ustawić dodatkowe, własne reguły dotyczące na przykład konkretnego adresu IP czy URL.

SERWER DNS

DNS (Domain Name System) to system, który tłumaczy zrozumiałe dla ludzi adresy stron internetowych (URL) na odpowiadające im adresy IP, które są zrozumiałe dla komputerów. Na przykład adres https://bezpieczny.blog zostanie przetłumaczony na adres 104.21.57.111. Urządzenie podłączone do sieci (także twój router) ma zapisany w konfiguracji adres IP serwera DNS i prosi ten serwer o tłumaczenie adresów. Zmiana adresu serwera DNS może przyczynić się do poprawienia bezpieczeństwa. Niektóre serwery DNS mogą na przykład blokować translacje adresów do znanych złośliwych stron, jak to robi serwer Quad9 dostępny pod adresem 9.9.9.9. O tym, jak stworzyć własny serwer DNS poprawiający nasze bezpieczeństwo, możesz przeczytać w artykule Łukasza Basy „Zabezpieczamy domową sieć przed stronami wyłudzającymi od nas dane" opublikowanego w numerze 1/2021 (09).

AKTUALIZACJE SYSTEMU

Aktualizacje systemów operacyjnych (nie tylko routerów) to podstawa, jeśli chodzi o higienę bezpieczeństwa. Trudno jednak wymagać od użytkownika, aby dla kilku urządzeń codziennie sprawdzał, czy została wydana kolejna aktualizacja. Dlatego niektórzy producenci udostępniają funkcję automatycznych aktualizacji. Po jej włączeniu twój router będzie automatycznie instalował poprawki o wyznaczonej godzinie (na przykład w nocy, gdy nikt nie korzysta z Internetu) bez konieczności interakcji.

QOS

Quality of Service (QoS) to w przypadku routerów zestaw reguł pozwalających na poprawienie działania

konkretnych usług w naszej sieci domowej. Router może na przykład przepuszczać ruch pochodzący z usług wideo (Netflix, YouTube, Disney+) przed ruchem z usług związanych z przeglądaniem stron internetowych albo wideorozmów. Wpływa to na płynność działania danej usługi. Często można też ustawić cały ruch z danego urządzenia jako ważniejszy niż z pozostałych w sieci. Poprawia to komfort użytkowania naszej sieci.

FILTROWANIE ADRESÓW MAC

Każda karta sieciowa, nieważne czy przewodowa, czy Wi-Fi, ma adres MAC (Media Access Control) i posługuje się nim, zanim uzyska adres IP. Można powiedzieć, że karta przedstawia się tym adresem routerowi. W założeniu adres ten powinien być unikalny i niezmienny. Dzięki filtrowaniu adresów MAC można określić, czy pozwolimy danemu urządzeniu na podłączenie się do sieci, czy też nie. W praktyce jednak karty lub mechanizmy systemu operacyjnego pozwalają na zmianę tej wartości. Powoduje to, że w dzisiejszych czasach mechanizm ten jest prosty do obejścia. Ponadto utrudnia to podłączanie nowych urządzeń, bo w każdym przypadku użytkownik musi dodać nowy adres MAC do konfiguracji filtrowania adresów MAC routera.

DHCP

DHCP (Dynamic Host Configuration Protocol) to protokół sieciowy pozwalający urządzeniom podłączającym się do naszej sieci na otrzymanie od routera danych konfiguracyjnych, na przykład przydzielonego adresu IP, adresu IP bramy sieciowej, adresu serwera DNS czy maski podsieci. Gdyby ten mechanizm wyłączyć, to nowe urządzenie nie podłączy się do sieci, chyba że powyższe informacje uzyskało już wcześniej (na przykład użytkownik wprowadził je ręcznie). Jeśli DHCP jest włączony w naszej sieci, to możliwe jest, że to samo urządzenie uzyska różne adresy IP za każdym razem, gdy podłączy się do sieci. Może to jednak być wadą. Powiedzmy, że mamy drukarkę sieciową, z której korzystają domownicy. W celu oszczędzania energii drukarka jest wyłączona, gdy nie jest potrzebna. Po ponownym włączeniu uzyska ona inny adres IP i komputery w sieci będą musiały jej szukać, gdy użytkownik będzie chciał coś wydrukować. Może to chwilę potrwać. Podobny, uciążliwy efekt może wystąpić przy urządzeniach IoT (Internet of Things) czy serwerach plików NAS (Network Attached Storage), na których przechowujemy pliki. Aby uniknąć tego efektu, możemy ustawić stały adres IP dla danego sprzętu – przy każdym podłączeniu do sieci router będzie przydzielał mu ten sam adres IP. Należy pamiętać, że takie przydzielenie adresu może nie zadziałać w przypadku, gdy urządzenie ma włączoną funkcję randomizacji adresów MAC (na przykład „Prywatny adres Wi-Fi" w systemie iOS).

CIEKAWOSTKA

Historycznie router to urządzenie sieciowe, które służy do łączenia oddzielnych sieci komputerowych (na przykład o różnych klasach adresów IP, maskach sieciowych). Trasuje (kieruje/routuje) ono pakiety sieciowe między siecią źródłową a docelową.

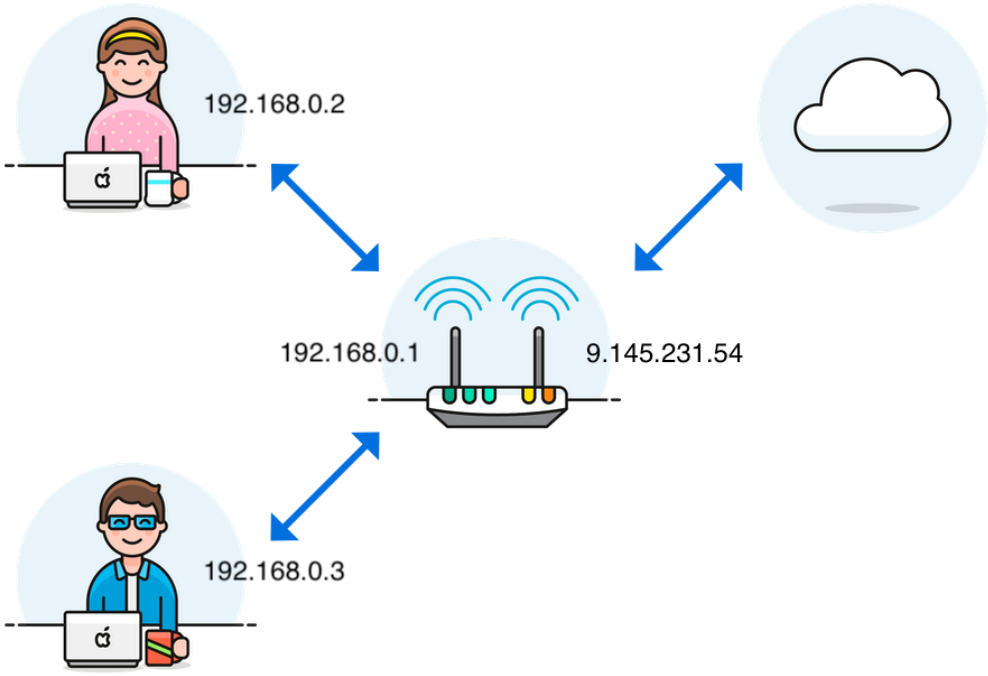
Tak zwane domowe routery to właściwie połączenie kilku różnych urządzeń: routera, przełącznika/switcha (kierowanie pakietami wewnątrz sieci domowej), punktu dostępowego Wi-Fi (zapewnianie dostępu do sieci bezprzewodowej) oraz czasem modemu (zapewnianie dostępu do sieci Internet).

BLOKADA DOSTĘPU DO INTERNETU

Jeśli mamy w sieci urządzenia, które nie są już wspierane przez producenta i nie dostają aktualizacji (na przykład stara drukarka sieciowa) lub takie, którym do końca nie ufamy (na przykład kolorowa żarówka LED sterowana przez Wi-Fi), to możemy je czasowo lub trwale odciąć od Internetu. Router będzie blokował wszelkie połączenia na zewnątrz od takiego urządzenia. W zależności od routera możemy zablokować ruch, korzystając z dedykowanej opcji lub tak zwanej kontroli rodzicielskiej.

NAT

Translacja adresów sieciowych (Network Address Translation, NAT) umożliwia zmianę źródłowych i docelowych adresów IP i portów sieciowych w pakietach podczas ich przekazywania między sieciami przez router. Pozwala to na ukrycie sieci domowej za jednym zewnętrznym adresem IP przypisanym do routera przez operatora – tak zwana maskarada IP (Ilustracja 1). W praktyce NAT umożliwia dostęp wielu urządzeniom w sieci lokalnej do zasobów Internetu poprzez



Ilustracja 1. Przykład zastosowania „NAT”

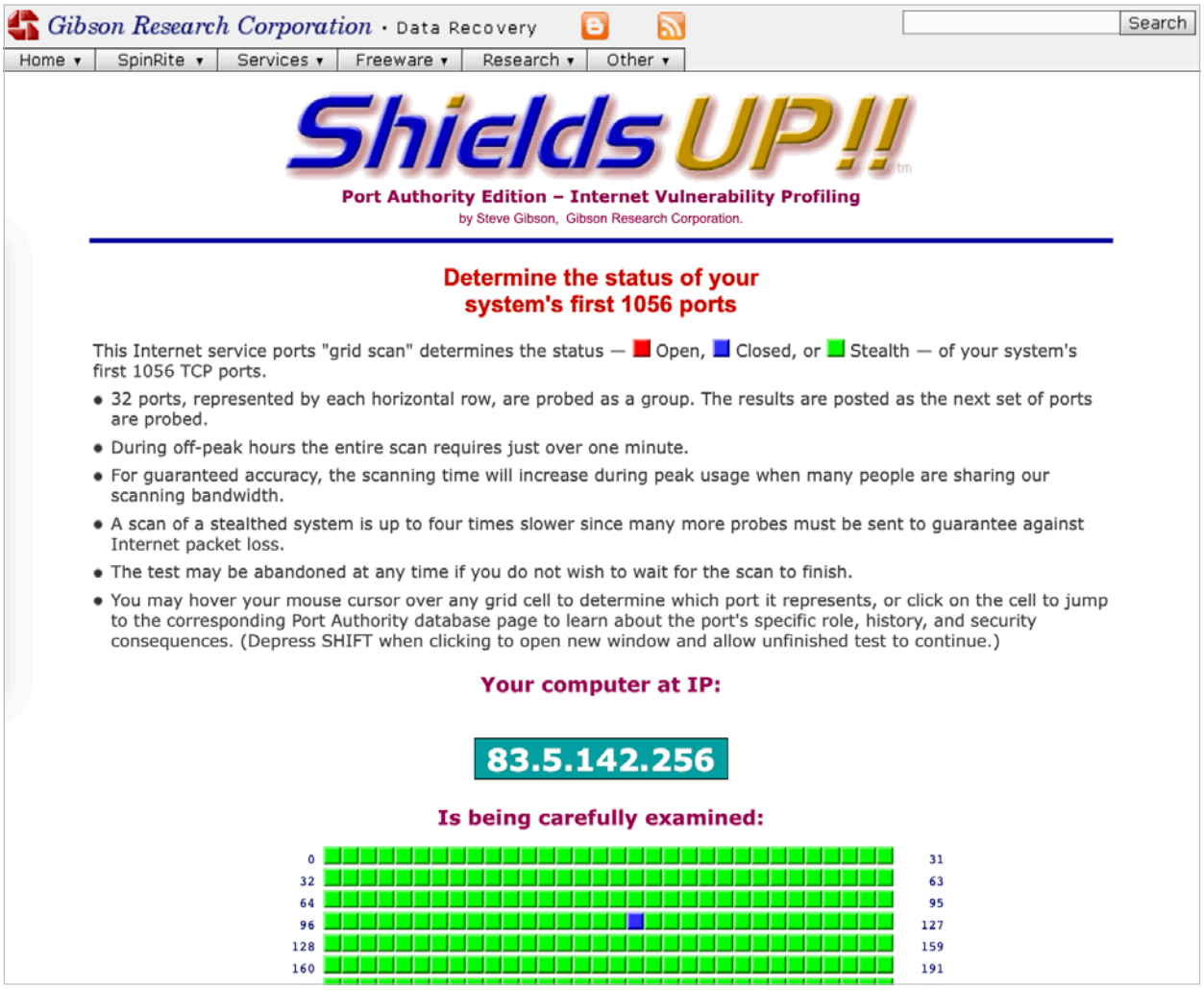
router. Mechanizm ten jest zazwyczaj domyślnie włączony. Jeśli jest włączony na modemie od operatora oraz na naszym routerze, to komputery w naszej sieci są za tak zwanym podwójnym NAT-em. Może on powodować konieczność wykonania dodatkowych kroków przy konfiguracji innych usług, na przykład DDNS (Dynamic Domain Name System).

PORT FORWARDING

Przekierowanie portów (ang. *port forwarding*) pozwala na przekierowanie pakietów przychodzących z Internetu na określony port routera do adresu IP i portu konkretnego urządzenia w sieci lokalnej. Przekierowanie może dotyczyć różnych protokołów. Umożliwia to komunikację z zewnątrz z urządzeniem wewnątrz naszej sieci, na przykład serwerem poczty lub konsolą do gier. Należy uważać przy konfiguracji tej opcji, gdyż może się okazać, że urządzenie z naszej sieci jest osiągalne z zewnątrz i może zostać łatwo zaatakowane. Na szczęście routery udostępniają listę zawierającą wszystkie przekierowania portów, co pozwala na łatwe sprawdzenie, czy nie wykonaliśmy przypadkowo niebezpiecznego kroku. Aby sprawdzić, jakie porty sieciowe (z 1056 pierwszych portów TCP) na naszym routerze są widoczne z sieci, można posłużyć się darmowym narzędziem ShieldsUP (Ilustracja 2), działającym w przeglądarce i dostępnym pod adresem https://www.grc.com/shieldsup.

UPNP

Mechanizm *Universal Plug'n'Play* (UPnP) powstał, aby ułatwić życie użytkownikom np. konsol do gier. Po podłączeniu do kompatybilnego routera konsola przekazuje routerowi konfigurację sieciową, jakiej potrzebuje ona do poprawnego funkcjonowania w sieci, na przykład udrożnienie ruchu na danym porcie sieciowym. W ten sposób użytkownik nie musi nic konfigurować na routerze, aby móc się cieszyć sieciowymi funkcjami konsoli, jak na przykład rozgrywką wieloosobową przez Internet. Ta funkcja ma jednak swoje wady. Dowolne urządzenie podłączone do naszej sieci może wpłynąć na konfigurację sieciową naszego routera bez naszego wyraźnego zezwolenia. Dodatkowo takie reguły sieciowe nie są widoczne w panelu administracyjnym routera. Możemy nawet nie wiedzieć, że żarówka LED sterowana przez Wi-Fi komunikuje się z nieznanym nam serwerem po niestandardowym porcie. Wspomniane już narzędzie ShieldsUP może także sprawdzić, czy protokół UPnP jest uruchomiony na naszym routerze (Ilustracja 3).



Ilustracja 2. Fragment wyniku skanowania portów za pomocą narzędzia „ShieldsUP”

DOSTĘP ADMINISTRACYJNY Z ZEWNĄTRZ

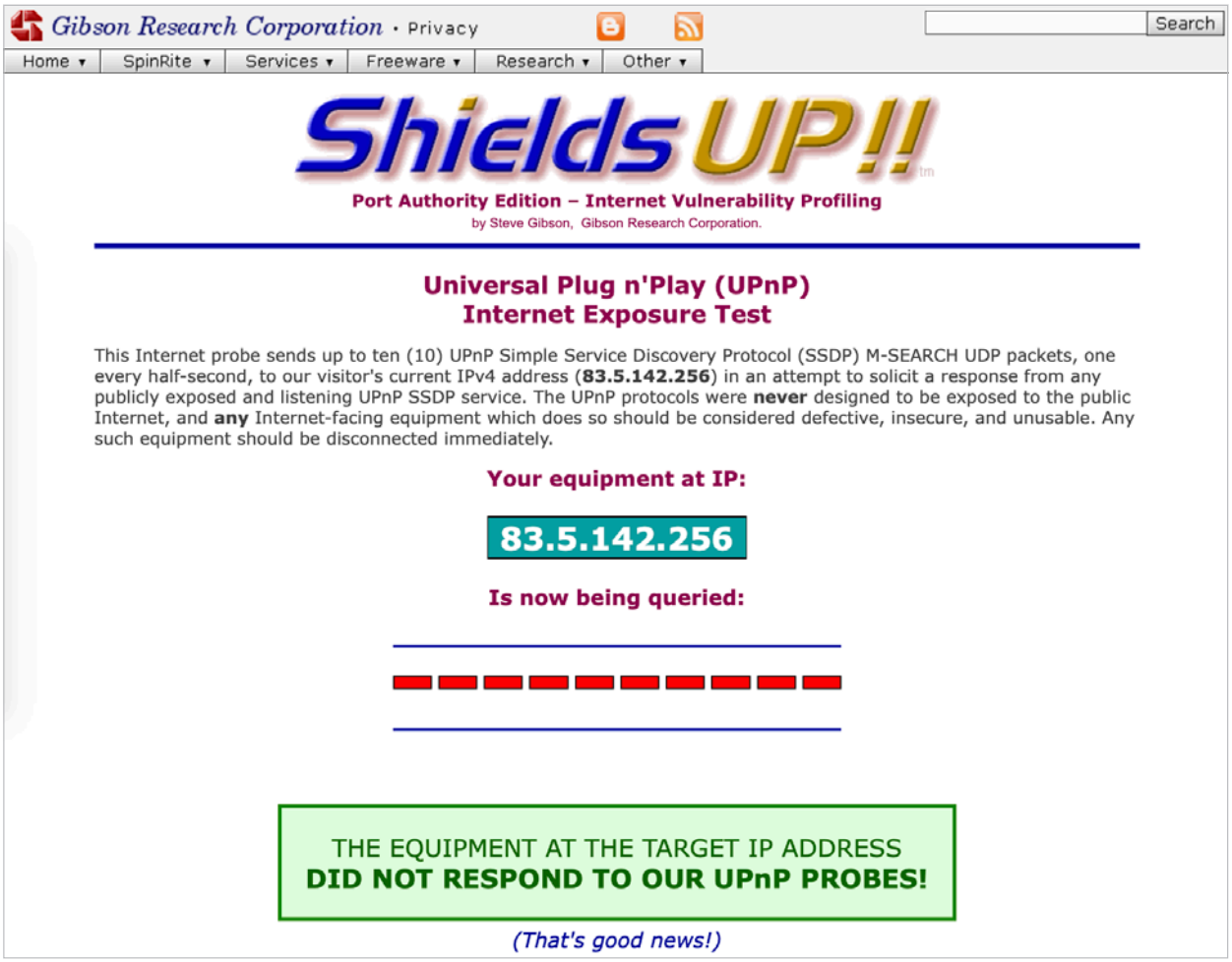
Niektóre routery pozwalają na dostęp administracyjny z zewnątrz. Bywa, że jest to włączone domyślnie, aby ułatwić życie użytkownikowi. Należy pamiętać, że to oznacza, iż w Internecie jest widoczna strona logowania do naszego routera i tylko ona chroni naszą sieć przed niepożądanymi zmianami przez atakującego. Jeśli nie mamy wyraźnej potrzeby, należy wyłączyć tę opcję. Jeśli istnieje potrzeba zdalnego zarządzania, to lepiej uruchamiać taki dostęp okresowo, w razie potrzeby lub ograniczyć dostęp do panelu logowania jedynie ze zdefiniowanych adresów IP. Jeśli pomagacie innym w zarządzaniu ich siecią zdalnie, to lepiej napisać im instrukcję, jak tę opcję włączyć, w razie gdy potrzebują waszej pomocy.

UKRYWANIE SSID

W dzisiejszych czasach ta funkcja raczej utrudnia użytkowanie sieci bezprzewodowej niż poprawia bezpieczeństwo. Niektóre urządzenia (jak drukarki) mogą mieć problem z podłączeniem się do takiej sieci, a istnienie takiej sieci i tak łatwo wykryć skanerem sieci bezprzewodowej (Ilustracja 4).

DODATKOWE SIECI WI-FI

Niektóre routery pozwalają na stworzenie dodatkowych sieci Wi-Fi, które są odseparowane od pozostałych sieci, czyli urządzenia podłączone do takiej sieci nie „widzą” tych w pozostałych sieciach. Może być to przydatne do stworzenia sieci Wi-Fi dla urządzeń niezaufanych, na przykład dla komórek naszych gości, komputerów służbowych/szkolnych czy sprzętów IoT, które czasem potrafią robić dziwne rzeczy, na przykład



Ilustracja 3. Przykładowy wynik sprawdzenia, czy mechanizm „UPnP" jest włączony, przy użyciu narzędzia „ShieldsUP"

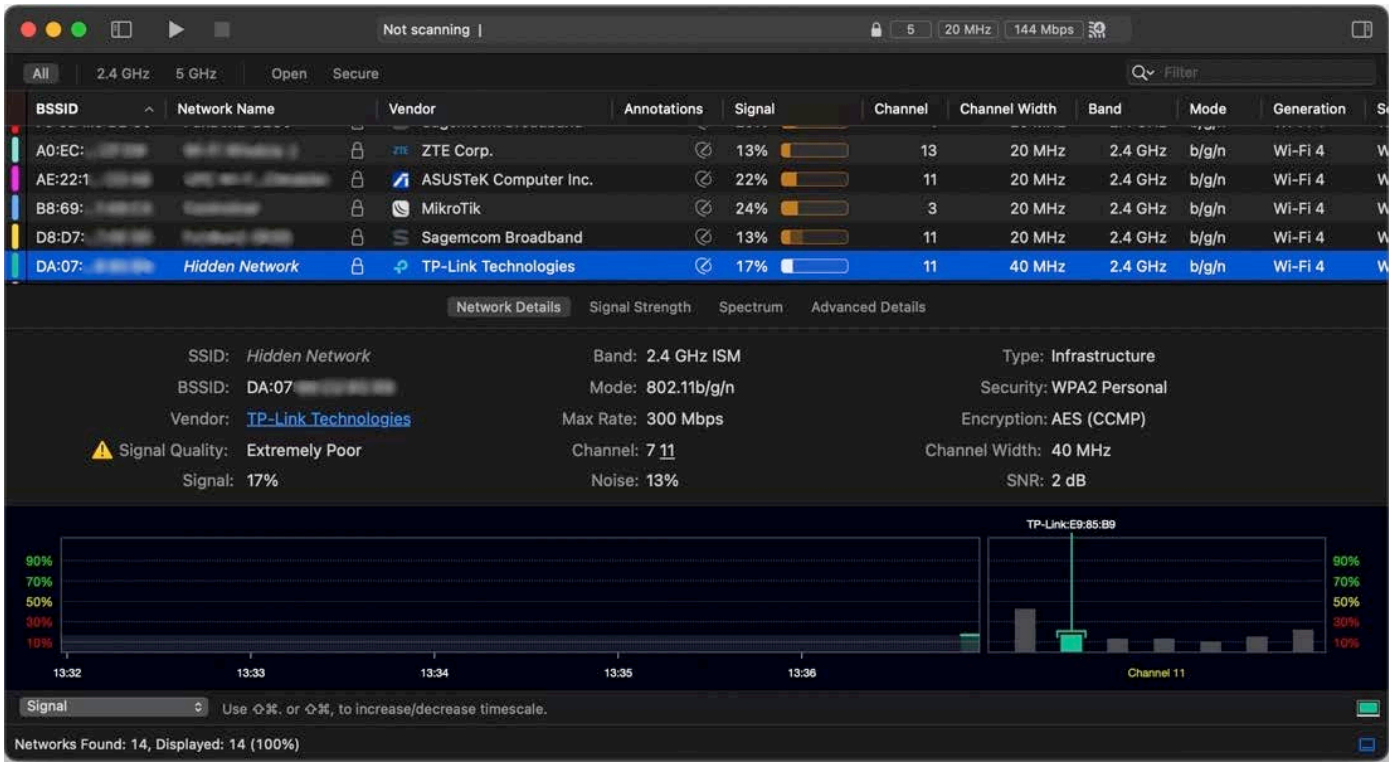
skanować naszą sieć domową i wysyłać wyniki do swojego producenta. Ponadto taka sieć może być skonfigurowana z ograniczeniem przepustowości, dostępu do Internetu czy czasowym wyłączeniem nadawania. Warto również ograniczyć dostęp do panelu administracyjnego routera z takich sieci.

WPA

Wi-Fi *Protected Access* (WPA) to standard zabezpieczeń w sieciach bezprzewodowych i następca WEP (Wired Equivalent Privacy). Występuje w trzech wersjach i jeśli to możliwe, należy korzystać z najnowszej wersji – 3. Poprawia ona błędy wcześniejszych wersji i podwyższa bezpieczeństwo sieci, lecz może nie być zaimplementowana w starszych urządzeniach. W takim przypadku trzeba korzystać z wcześniejszej wersji lub trybu mieszanego WPA2/WPA3.

WPS

Niektóre routery umożliwiają podłączenie urządzenia do sieci za pomocą mechanizmu Wi-Fi *Protected Setup* (WPS) bez potrzeby wprowadzania hasła do sieci bezprzewodowej przez użytkownika. Jest kilka wariantów tego mechanizmu. Jeden z nich polega na przyciśnięciu dedykowanego guzika na routerze (lub w interfejsie administracyjnym) oraz na urządzeniu (na przykład drukarce) w krótkim odstępie czasu. W ten sposób urządzenia wchodzą w tryb parowania i „dogadują" się w sprawie połączenia. Inny wariant polega na wprowadzeniu w konfiguracji routera specjalnego numeru PIN wygenerowanego przez urządzenie. W założeniu ten mechanizm miał uprościć dodawanie sprzętów do sieci, ale błędy implementacji pozwalały na ataki polegające na odzyskaniu tego PIN-u po podsłuchiwaniu ruchu sieciowego i dostaniu się do sieci. Myślę, że lepiej korzystać z dobrego hasła i wyłączyć ten mechanizm.



Ilustracja 4. Wynik działania narzędzia „Wi-Fi Explorer" pokazujący „ukrytą" sieć

PODSUMOWANIE

Jak widać, domowy router wcale nie jest tak prostym urządzeniem, jak mogłoby się to wydawać. Jego konfiguracja może przysporzyć kłopotów, jeśli nie rozumie się jego funkcji. Dlatego zanim zaczniesz zmieniać ustawienia routera, dowiedz się, jakie mogą być tego konsekwencje. Warto najpierw spróbować „na sucho" z routerem innym niż główny router w domu.

Marcin Gromek

Ekspert ds. bezpieczeństwa IT. Uwielbia słuchać podcastów i pić dobrą kawę. Pisze i nagrywa dla serwisu bezpieczny.blog.

KONTAKT@BEZPIECZNY.BLOG

ZAPAMIĘTAJ

- Wiele funkcji współczesnych routerów jest domyślnie włączona. Warto sprawdzić, czy nie powodują pogorszenia bezpieczeństwa naszej sieci.
- Dowiedz się, jak działa dana funkcja, zanim zmienisz jej ustawienia.
- Zmieniaj ustawienia pojedynczo, aby w razie czego wiedzieć, co spowodowało zmianę działania sieci.

ĆWICZ W DOMU

- Jeśli masz w domu nieużywany router, poćwicz najpierw na nim.
- Sprawdź konfigurację swojego routera. Być może możesz poprawić bezpieczeństwo swojej sieci domowej.

Wiktor Szymański

Znajdź wirtualną flagę

Kto z nas nie lubi zagadek? Przechodzenie labiryntów, łamanie szyfrów, rozwiązywanie rebusów czy znajdowanie różnic między obrazkami to czynności, które wymagają cierpliwości, skupienia oraz staranności. Stawiają wyzwanie, rozwijają umiejętność analitycznego myślenia oraz dają poczucie, że odpowiednie podejście pozwala uporać się z problemem, który na pierwszy rzut oka może wydawać się nierozwiązywalny. Coraz częściej jednak świat łamigłówek wypierany jest przez magię oferowaną przez świat cyfrowy. A gdyby tak dało się połączyć ze sobą oba te światy?

12+

DOWIESZ SIĘ

- Co to są zadania i konkursy CTF.
- Od czego rozpocząć naukę.
- Gdzie znaleźć przykładowe zadania CTF.

POTRZEBNA WIEDZA

- Dostęp do Internetu oraz dużo zapału i chęci do nauki.

CAPTURE THE FLAG (CTF)

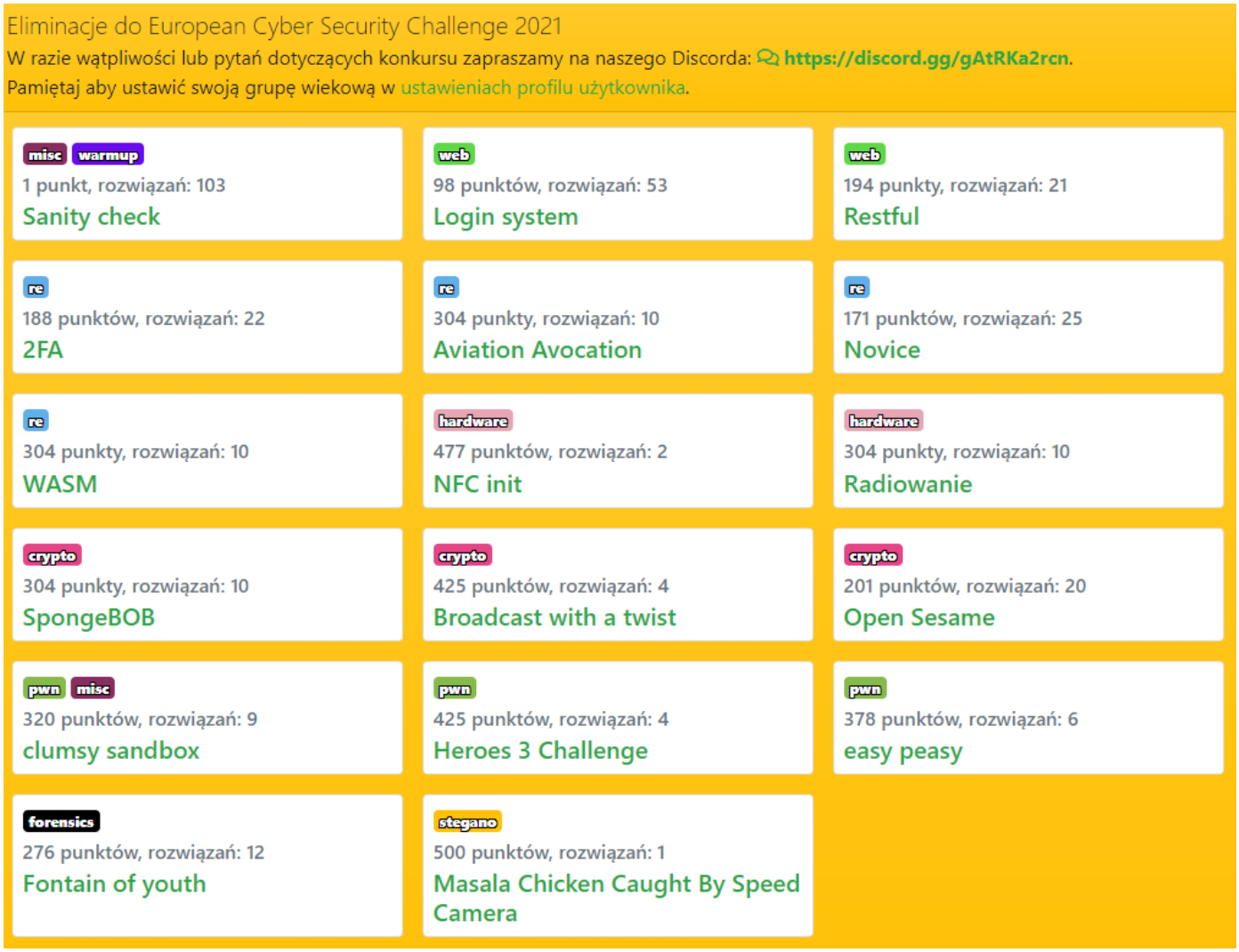
Na przełomie lat 90. i 2000 wielką popularnością cieszyły się gry typu FPS (ang. *First Person Shooter*), takie jak „Quake III Arena" czy „Unreal Tournament". Wówczas zwrot CTF (ang. *Capture The Flag*) kojarzył się z trybem rozgrywki zespołowej, w którym żeby wygrać rundę, jedna drużyna musiała zdobyć flagę drużyny przeciwnej określoną liczbę razy. Należało ją wykraść z bazy przeciwnika i przetransportować do lokalizacji kontrolowanej przez własną drużynę.

Zwrot CTF to również określenie dla zawodów/zadań, w ramach których uczestnicy muszą wykazać się znajomością i praktycznymi umiejętnościami w obszarze programowania, kryptografii i bezpieczeństwa aplikacji internetowych, by wykorzystując błędy w oprogramowaniu, rozwiązując programistyczne problemy i szukając logicznych wytrychów, odnajdywać ukryte przez twórców „flagi". Flaga to ukryty w cyfrowym zadaniu ciąg znaków o określonej długości stanowiących potwierdzenie, że zadanie zostało ukończone. Celem zawodów CTF jest popularyzacja wśród młodzieży i dorosłych zainteresowania tematyką cyberbezpieczeństwa. W trakcie konkursów uczestnicy w legalny sposób mogą zaspokoić ciekawość dotyczącą tego, jak to jest „być hackerem", przełamywać zabezpieczenia i obchodzić czy atakować systemy.

```
CTF{Th3r3_1s_4lw4y5_4N07h3r_W4y}
CTF{4ll_D474_5h4ll_B3_Fr33}
CTF{g00doldDOS-FTW}
```

Ilustracja 1. Przykład wartości flag występujących w konkursie Google CTF (capturetheflag.withgoogle.com). Wartość flag zapisana jest w popularnym formacie „CTF{ciąg_znakow}" (źródło: youtube.com/hashtag/pasjainformatyki)

Zadania CTF podzielone są na obszary tematyczne informujące użytkownika, jaka z dziedzin informatyki czy bezpieczeństwa informatycznego będzie kluczowa do rozwiązania danego zagadnienia. Mogą to być między innymi:



Ilustracja 2. Lista zadań CTF stworzona przez zespół Cert.pl w ramach eliminacji do wydarzenia European Cyber Security Challange

- programowanie,
- kryptografia,
- bezpieczeństwo aplikacji webowych,
- informatyka śledcza (ang. *computer forensics*),
- inżynieria wsteczna (ang. *reverse engineering*),
- mieszanie wszystkich kategorii (ang. *misc*).

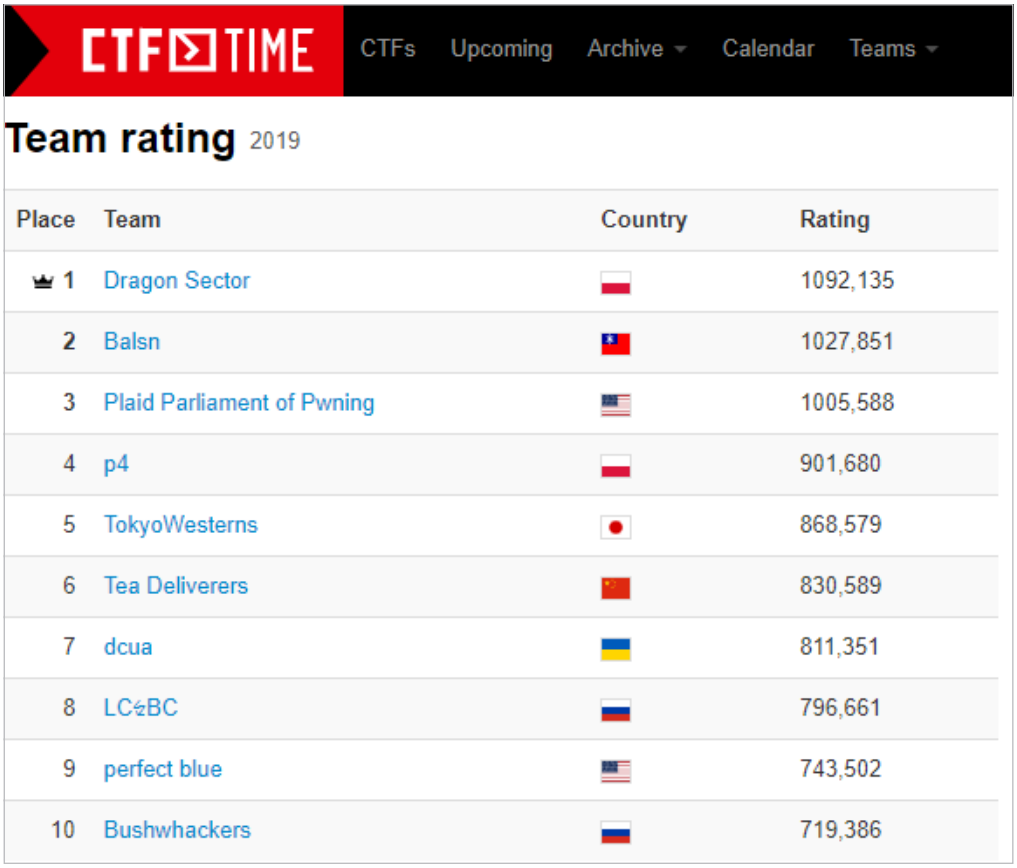
Zadania, oprócz przypisania do kategorii, zawierają również informacje o tym, ile punktów warta jest flaga – im więcej, tym zadanie jest trudniejsze do ukończenia, składa się z większej ilości etapów, które należy przejść, żeby ją znaleźć. Częstą praktyką jest zawieranie w tytule lub opisie zadania drobnych podpowiedzi dla użytkownika (na przykład w postaci aluzji lub od-

CIEKAWOSTKA

Instytut Wymiaru Sprawiedliwości organizuje ogólnopolski konkurs Capture The Flag „153+1". Przedsięwzięcie jest skierowane do uczniów publicznych i niepublicznych szkół ponadpodstawowych, w szczególności techników oraz szkół branżowych o profilu informatycznym. Konkurs został objęty honorowym patronatem Ministra Edukacji Narodowej. Każdego roku zapisy do konkursu rozpoczynają się w październiku lub listopadzie.

Na zwycięzców konkursu czekają atrakcyjne nagrody pieniężne.

Więcej informacji na stronie 153plus1.pl.



CTFTIME CTFs Upcoming Archive Calendar Teams

Team rating 2019

Place	Team	Country	Rating
1	Dragon Sector		1092,135
2	Balsn		1027,851
3	Plaid Parliament of Pwning		1005,588
4	p4		901,680
5	TokyoWesterns		868,579
6	Tea Deliverers		830,589
7	dcua		811,351
8	LC↯BC		796,661
9	perfect blue		743,502
10	Bushwhackers		719,386

Ilustracja 3. Polskie zespoły CTF w 2019 roku zakończyły rywalizację na wysokich pozycjach (źródło: CTFTime.org)

wołań do zagadnień kulturowych) mogących naprowadzić grającego na właściwe tory lub w sprytny sposób poinformować go o tym, od której strony ugryźć cyfrową zagadkę.

Popularne platformy z zadaniami CTF to:

- PICO CTF (picoctf.org),
- Beginners quest CTF with Google (capturetheflag.withgoogle.com/beginners-quest),
- Zadania CTF od zespołu cert.pl (hack.cert.pl/challenges).

WARTO WIEDZIEĆ

Warto prowadzić i aktualizować notatki z zadań CTF, które rozwiązujemy (wykorzystane narzędzia, metody, napisany kod, przydatne artykuły typu writeup). Będą one przydatne podczas rozwiązywania kolejnych zadań, zwłaszcza w trakcie konkursu, w którym czas na ich rozwiązanie jest ograniczony.

NIE OD RAZU RZYM ZBUDOWANO[1]

Nie przejmuj się, jeżeli po otworzeniu kilku przykładowych zadań CTF jesteś w kropce.

Jak w przypadku tradycyjnych zagadek i łamigłówek, nabycie biegłości w poruszaniu się po meandrach zadań CTF wymaga praktyki i ćwiczeń połączonych z wiedzą z zakresu informatyki oraz przestawieniem się na nieszablonowy sposób myślenia i podejścia do stawianych przed nami wyzwań. Jeżeli dopiero zaczynasz swoją przygodę ze zbieraniem wirtualnych flag, zachęcam do zapoznania się z playlistą Capture The Flag z kanału „Pasja Informatyki". Wiedzę możesz również zdobyć, analizując opis rozwiązań historycznych konkursów CTF (tak zwany writeup). Doskonałą bazą w tym zakresie jest blog (gynvael.coldwind.pl/) lub kanał platformie YouTube (www.youtube.com/user/GynvaelColdwind), który prowadzi Gynvael Coldwind.

1. Kraków zresztą też.

CIEKAWOSTKA

W 2021 roku reprezentacja Polski (złożona z osób pomiędzy 14 a 25 rokiem życia) zajęła 2 miejsce w corocznym konkursie European Cyber Security Challenge (tinyurl.com/2p9y8r3h).

Polskie zespoły biorące udział w międzynarodowych konkursach CTF (na przykład Dragon Sector czy P4) zajmują wysokie pozycje w międzynarodowym rankingu CTF (ctftime.org). Zespół Dragon Sector zakończył rok 2019 (oraz 2018) na 1. miejscu, a zespół P4 na 4. (a w 2018 roku na 3.). W roku 2020 obie drużyny znalazły się na liście Top10 najlepszych zespołów.

PRZED WYRUSZENIEM W DROGĘ NALEŻY ZEBRAĆ DRUŻYNĘ[2]

By doskonalić swoje umiejętności, zadania CTF można oczywiście rozwiązywać samemu w domowym zaciszu, jednak przystąpienie do konkursu CTF często wiąże się z przynależnością do zespołu. Głównym powodem takiego podejścia jest liczba zadań występująca w trakcie konkursu, mnogość zagadek z różnych obszarów bezpieczeństwa informatycznego oraz ograniczenie czasowe na znalezienie flagi.

Bycie częścią zespołu CTF to doskonała okazja do wymiany wiedzy z innymi osobami (zwłaszcza w obszarach, w których mamy mniej doświadczenia), poprawienie umiejętności pracy w grupie czy zdolności planowania i komunikacji. To również szansa na poznanie interesujących ludzi, którzy mają podobne do naszych zainteresowania.

2. Kultowy tekst z gry „Baldurs Gate".

Wiktor Szymański

Współzałożyciel serwisu bezpieczny.blog, fan LEGO, sympatyk dzielenia się wiedzą, maniak planszówek, miłośnik książek i filmów szpiegowskich. Na co dzień zajmuje się dbaniem o bezpieczeństwo aplikacji webowych.

KONTAKT@BEZPIECZNY.BLOG

!

ZAPAMIĘTAJ

- Capture The Flag (CTF) to rodzaj ćwiczenia/konkursu, w ramach którego uczestnik musi wykazać się znajomością i praktycznymi umiejętnościami w obszarze programowania, kryptografii i bezpieczeństwa internetowego. Rozwiązanie zadania zakończone jest uzyskaniem przez uczestnika tak zwanej „flagi".
- CTF writeup to szczegółowy opis rozwiązania zadania CTF zawierający informacje o sposobie podejścia do rozwiązania problemu oraz wykorzystanych technikach, które doprowadziły do odnalezienia flagi. Występują często w postaci wpisu na blogu.
- Nabycie biegłości w rozwiązywaniu zadań CTF wymaga praktyki i ćwiczeń.
- Zadania CTF można rozwiązywać samemu w domu, jednak przystąpienie do konkursu CTF często wiąże się z przynależnością do zespołu.

ĆWICZ W DOMU

- Spróbuj swoich sił, rozwiązując zadania z wykorzystaniem opisanych w artykule platform CTF.
- Regularnie czytaj artykuły typu CTF writeup dla historycznych zadań.
- Pogłębiaj swoją wiedzę z informatyki w obszarach, które cię interesują.
- Wraz ze znajomymi podejmijcie wyzwanie i zapiszcie się do udziału w ogólnopolskim konkursie CTF „153+1" objętym honorowym patronatem Ministra Edukacji Narodowej.

securitum

WYKONAJ AUDYT BEZPIECZEŃSTWA

CZYM JEST AUDYT BEZPIECZEŃSTWA? CZY MOJA ORGANIZACJA GO POTRZEBUJE?

Audyty to wykonywane na zlecenie firm i organizacji testy, które sprawdzają poprawność działania i bezpieczeństwo ich programów, stron www, platform itp. Dzięki audytowi dowiesz się czy dane i poufne informacje przekazane przez użytkowników systemów są bezpieczne, czy korzystanie z gry nie przyniesie więcej szkody niż rozrywki, czy program działa tak, jak zakładałeś.

Co się może stać gdy nie przeprowadzisz audytu?

Jeżeli przekazane przez użytkowników dane dostaną się w ręce cyberprzestępców to mogą wykorzystać zdobyte informacje do przejęcia profili i kont w mediach społecznościowych, uzyskać dostęp do karty płatniczej, podszyć się pod daną osobę w sieci. A Twoja firma straci wiarygodność.

Czy audyt zapewnia bezpieczeństwo?

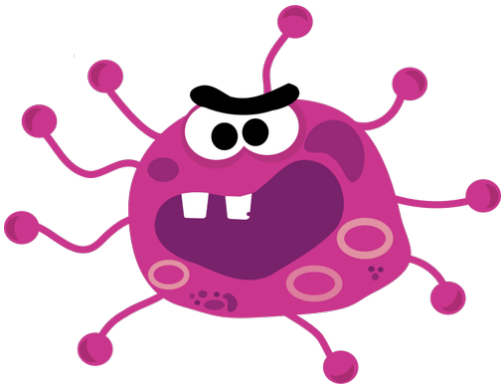
Przeprowadzając testy audytorzy sprawdzają działanie serwisu stosując podejście: gdybym chciał wykraść dane to... Znajdują słabe punkty w zabezpieczeniach – furtki, które mogą wykorzystać cyberzbóje, informują o nich i wspomagają proces ich zamykania.

SECURITUM.PL/AUDYTY

Jarosław Jedynak

Chory komputer, czyli rzecz o wirusach

Cyfrowy świat, podobnie jak ten za oknem, pełen jest niebezpieczeństw. Brak ostrożności podczas przebywania w Internecie może spowodować, że nasza maszyna zapadnie na komputerową chorobę. Skutki takiej infekcji są różne. Czasami komputer zaczyna działać wolniej, czasami otwierają się na nim same z siebie niepożądane okienka, ale często też nie obserwujemy niczego podejrzanego, a tymczasem właśnie wykradane są dane, hasła albo pieniądze. Warto nauczyć się kilku zasad, które pomogą ustrzec nasz sprzęt przed takim losem. W tym artykule omówimy przyczyny, skutki i sygnały wskazujące na to, że mamy problem.



Ilustracja 1. Wirus komputerowy. Wizja artysty

WIRUSY, ROBAKI I INNE PASOŻYTY

W świecie rzeczywistym choroby powstają, kiedy zarazki atakują zdrowe komórki. Podobnie jest w świecie wirtualnym – takie zarazki nazywamy „złośliwym oprogramowaniem" albo po angielsku „malware". Jest to ogólna nazwa na wszystkie rodzaje programów, które chcą wykorzystać nasz komputer w złym celu. Jak mówi stare przysłowie, żeby pokonać wroga, trzeba go najpierw poznać. Z tego powodu ludzie podzielili *malware* na różne kategorie i typy. Pierwszym podziałem jest klasyfikacja według sposobu infekcji:

1. Robaki – rozprzestrzeniają się szybko przez Internet, wykorzystując tak zwane eksploity[1]. Tak działał na przykład WannaCry (Ilustracja 2), który wykorzystywał eksploit EternalBlue, żeby przenosić się między komputerami z Windowsem bez najnowszych aktualizacji. Dlatego tak ważne jest regularnie instalować łatki bezpieczeństwa (zazwyczaj komputer robi to automatycznie).
2. Trojany (konie trojańskie) – udają inny program (np. ciekawą grę), ale po uruchomieniu pokazują swoje prawdziwe oblicze. Na przykład użytkownik może pobrać aplikację, która udaje zwykłą latarkę, ale tak naprawdę po zainstalowaniu zaczyna czytać wszystkie SMSy i wysyłać je na serwery przestępców.
3. Wirusy – dopisują swój kod do innych plików wykonywalnych na komputerze. W ten sposób szybko wszystkie programy na dysku są zarażone i jedynym ratunkiem jest reinstalacja wszystkiego. Kiedyś były popularne, ale dzisiaj prawie już nie występują. Mimo to z przyzwyczajenia czasami (błędnie) mówi się „wirus" na wszystkie rodzaje *malware*.
4. Oraz „inne", bo trafiają się przypadki, które w ogóle nie należą do żadnej z tych kategorii.

Jest to jednak problematyczne, bo za często coś nie pasuje do żadnej kategorii. Poza tym tak naprawdę ludzi interesuje, co taki złośnik robi, a nie, jak znalazł się na komputerze. Dlatego współcześnie dzielimy według sposobu działania:

1. Trojany bankowe (albo potocznie „bankery") wykradają pieniądze z kont użytkowników komputera logujących się do banku.
2. Ransomware (z ang. *ransom* – okup) szyfrują wszystkie pliki na dysku i żądają okupu (setek lub tysięcy złotych) za odszyfrowanie ich.

1. Eksploit to krótki program wykorzystujący błąd w oprogramowaniu, aby zyskać większe uprawnienia albo przejąć kontrolę nad systemem. Jeśli zostanie użyty na usłudze na innym komputerze w sieci, pozwala infekcji przenosić się przez Internet.

Ilustracja 2. WannaCry w akcji. Takie okienko wyświetlało się ludziom, którzy na swoje nieszczęście zostali zaatakowani (źródło: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

3. Spamboty wykorzystują komputery ofiar, żeby wysyłać spam (niechciane wiadomości e-mail).
4. Stealery (albo inaczej *spyware*) podsłuchują wpisywane hasła i wysyłają je do swoich twórców. Na takie konta logują się później nieznajomi i podszywają się pod prawdziwego użytkownika – mogą w ten sposób nieźle namieszać.
5. RATy (z ang. *Remote Access Trojan*, jest to kombinacja słów „trojan" i „zdalny dostęp") pozwalają obcej osobie zalogować się na komputer albo podglądać to, co dzieje się na monitorze w danym momencie.
6. I kilka innych...

W praktyce nowoczesne złośliwe oprogramowanie często należy do kilku kategorii jednocześnie. Ma dzięki temu więcej możliwości działania.

Znajomość takiego słowniczka bardzo pomaga w czytaniu artykułów o bezpieczeństwie IT albo rozmawianiu na ten temat. Ale sam podział złośliwego oprogramowania na kategorie nie pomoże nam wiele, jeśli zostaniemy nim zarażeni. Dlatego musimy nauczyć się, jak się przed nim uchronić.

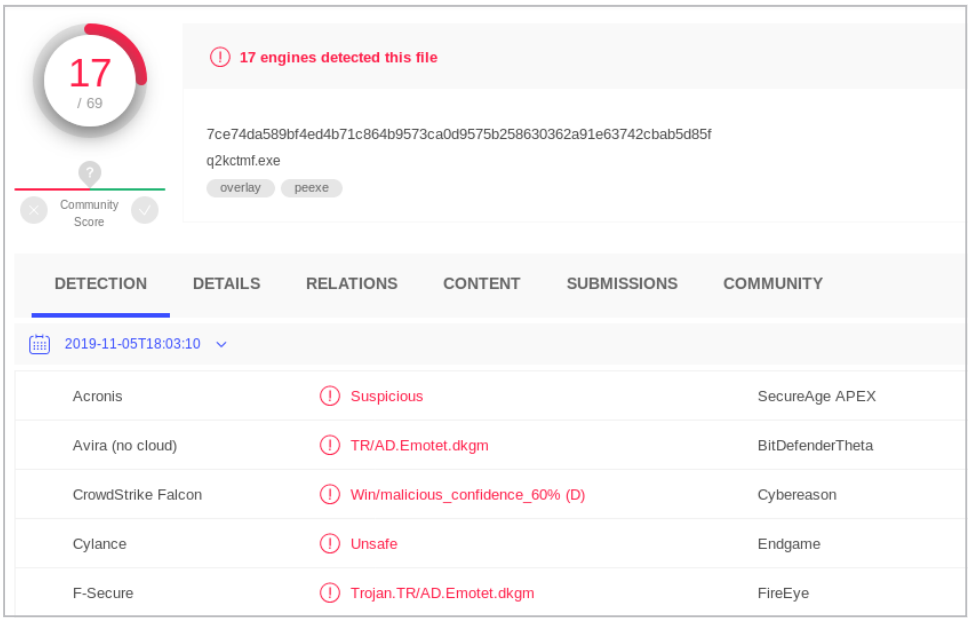
CIEKAWOSTKA

Czemu na złośliwe oprogramowanie udające przydatny program mówi się „koń trojański"? Legenda głosi, że podczas wojny trojańskiej Achajowie oblegali Troję, ale nie mogli przedostać się przez jej mury. Uciekli się więc do sposobu – zbudowali wielki drewniany posąg konia, schowali się w nim i zostawili go przed murami. Obrońcy wciągnęli posąg do miasta, myśląc, że to prezent, a tymczasem w nocy Achajowie wyszli z „konia trojańskiego" i podbili Troję. Stąd „koń trojański" to określenie na podstępny podarunek przynoszący zgubę obdarowanemu.

HIGIENA PRZY KOMPUTERZE

Przed wirtualnymi zarazkami zabezpieczymy się tak samo jak przed tymi materialnymi – zachowując odpowiednie zasady higieny. Nie chodzi tu o mycie rąk po wyjściu z ubikacji. Zasady higieny pracy przy komputerze są zupełnie inne, ale równie ważne.

Najważniejsza zasada to pobieranie programów tylko z zaufanych źródeł. Dla ludzi rozprowadzających złośliwe oprogramowanie nie ma nic prostszego,



Ilustracja 3. Interfejs systemu VirusTotal po wrzuceniu do niego złośliwego oprogramowania

niż wrzucenie złośliwego programu i nazwanie go np. „Fortnite.exe". Niczego nie spodziewająca się ofiara pobierze taki plik i uruchomi, infekując swoją maszynę. Jest to częsty scenariusz w przypadku tzw. cracków do gier. Osoba pobierająca i instalująca taki program często liczy się z tym, że jest trochę „nielegalny" i ignoruje ostrzeżenia antywirusa. Z tego powodu jest to łatwy sposób na ukrycie czegoś naprawdę złośliwego – bo jest duża szansa, że potencjalna ofiara uruchomi go mimo ostrzeżeń. Najbezpieczniej jest kupować programy zawsze tylko w sklepie, pobierać przez zaufanego dystrybutora (np. Steam lub Google Play) albo z oficjalnej strony producenta. Czasami jednak coś, czego szukamy, jest dostępne tylko przez mniej zaufane źródła – np. na anonimowej stronie internetowej albo serwisach wymiany plików typu torrent. Koniecznie trzeba wtedy zachować szczególną ostrożność. Na przykład, jeśli pobieramy film[2], a nazwa pliku kończy się na `.exe`[3], możemy być prawie pewni, że to koń trojański. Niebezpiecznych rozszerzeń jest więcej.

Ważne też jest ostrożne obchodzenie się z plikami otrzymanymi od kogoś w Internecie – przez e-mail albo nawet od znajomego. Często traktujemy je jako godne zaufania, tymczasem złośliwe załączniki to jedna z najpopularniejszych metod zarażania ludzi. Niektóre typy spambotów[4] są jeszcze bardziej złośliwe i potrafią podszywać się pod naszych znajomych albo ludzi, z którymi kiedyś korespondowaliśmy. Warto o tym pamiętać, kiedy ktoś, z kim dawno nie pisaliśmy, wyśle dziwną wiadomość, w której zachęca nas do zainstalowania czegoś albo wejścia pod jakiś link[5]. Z drugiej strony nie ma co wpadać w panikę – odbieranie zdjęć i filmów od osób, z którymi codziennie rozmawiamy, jest OK i nie grozi niczym złym.

Co zatem zrobić, jeśli chcemy uruchomić jakieś oprogramowanie, ale nie jesteśmy w 100% pewni, czy jest bezpieczne? Dobrą opcją jest przeskanowanie go za pomocą portalu VirusTotal (Ilustracja 3).

VirusTotal[6] sprawdza plik za pomocą kilkudziesięciu silników antywirusowych i pokazuje wynik w oknie przeglądarki. Jeśli pojawi się dużo czerwonych detekcji, oznacza to, że lepiej dać sobie spokój i zrezygnować z uruchamiania. Jeśli za to wyniki są w większości puste, program jest niemal na pewno bezpieczny.

2. Dodamy, że pobieranie za pomocą torrentów materiałów, do których nie mamy praw autorskich, jest zazwyczaj nielegalne i nie polecamy tego.

3. .exe to rozszerzenie, które w systemie Windows jest przypisane programom wykonywalnym.

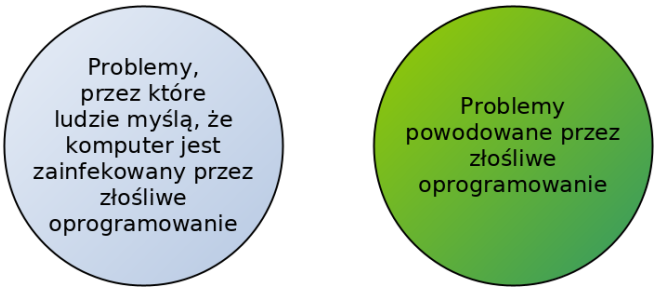
4. Przypomnienie: spambot to gatunek złośliwego oprogramowania, który wysyła spam – czyli niechciane wiadomości e-mail, które infekują kolejne maszyny.

5. Czy samo wejście na stronę może być szkodliwe? Wbrew pozorom – tak. Czasami w przeglądarkach internetowych trafiają się błędy pozwalające stronie na wykonanie dowolnego kodu na naszym komputerze (patrz też przypis o eksploitach). Jeśli regularnie aktualizujemy software, to ryzyko jest niewielkie, ale warto o tym pamiętać przed kliknięciem w podejrzany link.

6. Dostępny za darmo na stronie https://www.virustotal.com.

OBJAWY CHOROBY

Po czym poznać, że nasz komputer jest zawirusowany? Wbrew pozorom jest to dość trudne. Często ludzie wyobrażają sobie, że taki komputer musi zawsze działać powoli albo wyświetlać groźne komunikaty na ekranie. To nieprawda – zazwyczaj złośliwe skrypty starają się jak najlepiej ukryć w systemie i nie dawać znaku życia (Ilustracja 4).



Ilustracja 4. Dwa rodzaje problemów z komputerami – te, które są powodowane przez malware, i te, które wyglądają, jakby były spowodowane przez malware

Z tego powodu bardzo ciężko je wykryć, kiedy już dostaną się na nasz system. Dlatego ważne jest, żeby ich tam nie wpuścić. Najważniejsza jest ostrożność, jak pisaliśmy w poprzednim punkcie. Dodatkowo warto jest mieć cały czas włączony antywirus – dedykowany system do wykrywania i walki ze złośliwym oprogramowaniem. Co jakiś czas można też ręcznie skanować system, żeby sprawdzić, czy na pewno nie pojawiło się coś podejrzanego.

METODY LECZENIA

Najprostszą i najpewniejszą metodą usunięcia złośliwego oprogramowania jest przeniesienie ważnych danych (i tylko danych) na inny nośnik oraz ponowna instalacja systemu operacyjnego. Daje to największą pewność, że uda się usunąć zagrożenie, a przy okazji ciężko jest o czymś zapomnieć.

Jest to niestety dość czasochłonna metoda. Warto jednak to zrobić, bo skutki choroby mogą być poważne. Jeśli jednak bardzo zależy nam na czasie, bardzo wierzymy w swoje umiejętności albo po prostu chcemy poćwiczyć obchodzenie się z wirusami, możemy spróbować zrobić to ręcznie. W tym celu można pobrać skaner od firmy antywirusowej (albo skorzystać z wbudowanego Windows Defendera) i przeskanować system. Dla odważnych opcją jest analiza ręczna: warto użyć narzędzia *autoruns* napisanego przez pracownika Microsoftu[7]. Wyświetla ono wszystkie programy, które uruchamiają się przy starcie systemu. Jeśli faktycznie jesteśmy zainfekowani malwarem, będzie on na tej liście. Można przejrzeć ją całą i usunąć wszystkie podejrzane wpisy. Trzeba tylko uważać, żeby nie usunąć przypadkowo niczego potrzebnego – może to skończyć się uszkodzeniem systemu!

WARTO WIEDZIEĆ

Prawie każdy wie, że pliki .exe to programy. Ale nie każdy wie, że wykonywalnych rozszerzeń w systemie Windows jest znacznie więcej, między innymi:

- `.bat`: skrypty bat pochodzące jeszcze z czasów systemu DOS.
- `.ps1`: skrypty nowego typu, w języku Powershell
- `.jse`, `.js`, `.jsf`: skrypty JavaScript albo JScript
- `.vbs`, `.vbe`: skrypty w języku Visual Basic
- `.scr`: wygaszacze ekranu (to też programy!)

Na każdy plik z takim rozszerzeniem wystarczy kliknąć dwukrotnie myszką, żeby uruchomił swój kod na naszej maszynie.

PODSUMOWANIE

Złośliwe oprogramowanie to trudne, ale interesujące zagadnienie. Warto trochę o nim wiedzieć, żeby uchronić nasz system przed kataklizmem. Zainteresowanych tą problematyką zachęcamy do zgłębiania jej na własną rękę. Taka pasja może po kilku latach przerodzić się w dobrze płatną pracę, bo analiza złośliwego oprogramowania to ciągle ważny i potrzebny temat. A nawet jeśli nie planujemy zajmować się tą dziedziną zawodowo, taka wiedza na pewno się nam przyda.

7. https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

Jarosław Jedynak

Analityk malware w CERT Polska. W swojej pracy zajmuje się głównie walką ze złośliwym oprogramowaniem oraz przestępcami internetowymi. W wolnym czasie gra w CTFy z zespołem p4 albo rozwija własne projekty programistyczne.

MSM@TAILCALL.NET

Gynvael Coldwind

Etyczni hakerzy

Ze słowami „haker” i „haking” związanych jest równie wiele mitów co nieporozumień. W tym artykule postaram się wyjaśnić źródło zamieszania, a także wytłumaczyć, kim są etyczni hakerzy, jak i wskazać, jak nie wpaść w kłopoty, interesując się hakingiem. Chciałbym też zachęcić do przeczytania tego artykułu wspólnie z rodzicami lub opiekunami.

Zacznijmy od tego, że słowo „haker” ma kilka różnych definicji.

W języku potocznym „haker” jest w zasadzie synonimem „cyberprzestępcy”, a więc jest kojarzony z wykradaniem danych z serwerów, pieniędzy z kont bankowych czy przejęciem kont społecznościowych. Od razu zaznaczę, że nie jest to poprawna definicja, ale język potoczny rządzi się własnymi prawami.

W środowiskach informatycznych funkcjonują dwa lepsze terminy.

HAKER – AUTORYTET W TECHNICE

Dla programistów i elektroników hakerem jest osoba, która posiada ogromną wiedzę o tym, jak elementy systemów/programów działają od podszewki, i która umie w sposób kreatywny tą wiedzę wykorzystać. Z kulturą hakerską często wiążą się takie cechy jak chęć poznania, jak dany element systemu działa i jest zbudowany, chęć doprowadzenia danej technologii do granic jej możliwości (patrz również: demoscena) czy użycie urządzeń lub technologii w niestandardowych celach (częstym przykładem jest uruchomienie historycznie popularnych gier komputerowych na aparatach fotograficznych, drukarkach czy oscyloskopach). Tysiące fascynujących projektów hakerów można znaleźć na serwisie newsowym https://hackaday.com/.

Z uwagi na dużą rozbieżność powyższej definicji z językiem potocznym czasami w mediach możemy znaleźć zabawne pomyłki, jeśli dziennikarze nie są świadomi istnienia tego rozróżnienia. Często wskazywanym przykładem (który można znaleźć np. na Wikipedii) jest opublikowany w magazynie „Fortune” artykuł „Kto jest kim u hakerów” (ang. A *who's who of hackers*) autorstwa Shelley DuBois, który był poświęcony hakerom w potocznym tego słowa znaczeniu:

> *Niektórzy członkowie społeczności hakerskiej ostatecznie decydują się znaleźć zatrudnienie w korporacjach. Przykładowo, Linus Torvalds, człowiek, który stworzył centralny komponent systemu operacyjnego Linux, ma godną poszanowania historię w hakingu.*[1]

Oczywiście Linus Torvalds nigdy nie miał nic wspólnego z cyberprzestępcami, a nazywany jest hakerem z uwagi na swoją ogromną praktyczną wiedzę na temat systemów operacyjnych.

Zatrzymując się jeszcze na chwilę przy powyższej definicji, warto też wspomnieć o dwóch pokrewnych hasłach:

Pierwszym z nich jest „hack” jako określenie na niestandardowy kawałek kodu programu, który często łączy cechy bycia nieczytelnym ze sprytnym podejściem do rozwiązania danego problemu. Popatrzmy na przykład czytelnej implementacji funkcji signum dla liczb bez znaku (język C/C++):

```
unsigned int usgn(unsigned int v) {
  if (v == 0) {
    return 0;
  }
  return 1;
}
```

1. „Some members of this breed of hacker eventually go corporate. For example, Linus Torvalds, the man who wrote the central component for the Linux operating system, has a well-respected hacking history.”

WARTO WIEDZIEĆ

Filmy i seriale telewizyjne często prezentują haking jako serię – często trójwymiarowych – animacji, a cały pokazany proces zajmuje co najwyżej kilka minut. W praktyce haking niestety nie jest tak widowiskowy i najczęściej sprowadza się do wielogodzinnej pracy z dwukolorową konsolą tekstową.

Ilustracja 1. Kadr z filmu „Hakerzy" (1995, dystr. MGM United Artists)

Oraz na drugą, równoważną implementację, która sprytnie wykorzystuje sposób działania negacji logicznej w połączeniu z niejawnymi rzutowaniami pomiędzy typami `bool` i `unsigned int`, ale która zdecydowanie zasługuje na miano hacku:

```
unsigned int usgn(unsigned int v) {
  return !!v;  // Please excuse the hack.
}
```

Drugim powiązanym hasłem jest „hackerspace" – czyli lokalne laboratorium/warsztat działające zazwyczaj jako organizacja pozarządowa i służące jako miejsce spotkań, wymiany wiedzy i pracy nad wspólnymi projektami dla osób zainteresowanych elektroniką i informatyką. Listę hackerspace'ów znajdujących się na terenie Polski można znaleźć na stronie: https://wiki.hackerspaces.org/Poland.

HAKER – SPECJALISTA DS. BEZPIECZEŃSTWA KOMPUTEROWEGO

Wracając do próby zdefiniowania słowa „haker", przejdźmy do ostatniej istotnej dla nas[2] definicji: hakerem jest osoba, która ma wiedzę i umiejętności z dziedziny bezpieczeństwa komputerowego. W przeciwieństwie jednak do potocznej definicji samo określenie jest neutralne i często używane w stosunku do tzw. etycznych hakerów, czyli osób hobbystycznie i/lub zawodowo zajmujących się bezpieczeństwem komputerowym w pełni legalnym zakresie.

Historycznie można było również spotkać określenie „cracker" używane w stosunku do „złych hakerów" – trzeba tu jednak zaznaczyć, że w Polsce to określenie nigdy nie funkcjonowało, a zamiast tego „crackerami" nazywano osoby zajmujące się „software crackingiem", czyli sztuką przełamywania zabezpieczeń anty-piracckich (co samo w sobie również jest nielegalne w większości krajów, w tym w Polsce od roku 1994).

Współcześnie częściej można spotkać określenia związane z kolorami kapeluszy – tak więc etycznych hakerów przyjęło się nazywać białymi kapeluszami (ang. *white hat*), osoby działające na granicy prawa szarymi kapeluszami (ang. *gray hat* lub *grey hat*), a znanych z języka potocznego cyberprzestępców czarnymi kapeluszami (ang. *black hat*). Co ciekawe, jedną z największych konferencji poświęconych etycznemu hakingowi jest odbywający się w Las Vegas „Black Hat".

Warto zwrócić uwagę, że w praktyce zajmowanie się bezpieczeństwem wymaga bardzo dużej wiedzy o tym, jak programy – a wręcz całe systemy komputerowe – działają od podszewki, więc definicja ta nie

2. W słownikach możemy znaleźć jeszcze kilka innych definicji, takich jak „kierowca taksówki" lub „niedoświadczony golfiarz" (https://en.wiktionary.org/wiki/hacker#English).

jest specjalnie odległa od tej używanej w środowiskach programistycznych.

CZY WŁAMANIE MOŻE BYĆ ETYCZNE?

Po pierwsze, trzeba wyjaśnić, że bezpieczeństwo komputerowe to nie tylko włamania do systemów komputerowych, ale również np. kwestie zabezpieczeń przed włamaniami, bezpieczeństwa przesyłu i przechowywania informacji (kryptografia i kryptoanaliza) czy choćby wspomnianych wcześniej zabezpieczeń anty-pirackich – bezpieczeństwo komputerowe jest bardzo szeroką dziedziną. Niemniej jednak najczęściej haking faktycznie kojarzony jest z włamaniami do sieci lub systemów komputerowych.

Odpowiedź na powyższe pytanie brzmi: Tak – ale tylko w kilku bardzo konkretnych sytuacjach.

Zdecydowanie najważniejszą zasadą etycznego hakingu jest **posiadanie zgody właściciela systemu komputerowego na przeprowadzenie jakichkolwiek testów bezpieczeństwa**, a także **trzymanie się ściśle wyznaczonych reguł i granic** wyznaczonych przez prawo oraz ustalanych indywidualnie dla każdego przypadku. Co więcej, **zawsze musimy poinformować właściciela testowanego systemu o wszystkich znalezionych błędach**. Oprócz tego **zawsze należy szanować prywatność innych osób** i **nigdy nie należy dążyć do wyrządzenia szkody** – stąd też np. ataki klasy *Denial of Service* (pl. dosłownie *odmowa usługi*)[3] prawie nigdy nie są częścią testów bezpieczeństwa.

W praktyce powyższe zasady spełnione są jedynie w kilku przypadkach, takich jak testowanie bezpieczeństwa własnego komputera lub sieci, testy penetracyjne, red-teaming, bug bounty czy zawody e-sportowe i dedykowane serwisy do ćwiczenia umiejętności. W kolejnych sekcjach postaram się wyjaśnić niektóre z tych enigmatycznie brzmiących aktywności.

ZAWODOWY HAKING

Jedną z najlepszych metod sprawdzenia, czy nasze systemy komputerowe są bezpieczne, jest próba włamania się do nich, korzystając dokładnie z tych samych metod i technik, którymi mogą się posłużyć potencjalni cyberprzestępcy. I tym właśnie zajmują się pentesterzy wykonujący testy penetracyjne, a także specjaliści pracujący w tzw. red teamach (pl. dosłownie *czerwona drużyna*). W pewnym uproszczeniu różnica między nimi polega na tym, że pentesty są wykonywane przez zewnętrzne firmy specjalizujące się w usługach tego typu dla różnych firm, a red teamy są wewnętrznymi działami w danej firmie i interesuje je jedynie testowanie zabezpieczeń ich własnej firmy.

W ciągu kilku ostatnich lat bardzo popularne stały się również tzw. *bug bounty* (pl. dosłownie *nagrody za błędy*), czyli oferowane przez twórców oprogramowania oraz usługodawców nagrody pieniężne za wskazanie błędów bezpieczeństwa w ich aplikacjach lub serwisach internetowych. Bug bounty oferowane są m.in. przez największe firmy IT na świecie, takie jak np. Google, Facebook czy Microsoft, a przyznawane nagrody za najpoważniejsze błędy dochodzą do kilkuset tysięcy złotych. Listę programów bug bounty można znaleźć na dwóch poniższych stronach (choć trzeba zaznaczyć, że większość programów dopuszcza do udziału jedynie osoby pełnoletnie):

- https://www.bugcrowd.com/bug-bounty-list/
- https://www.hackerone.com/

W przypadku bug bounty kluczowym jest, aby trzymać się granic wyznaczonych przez organizatora.

HACKME, WARGAMES I CTF

Wcześniej wspomniałem, że haking wymaga ogromnej wiedzy – zarówno ogólnej z informatyki, programowania czy systemów komputerowych, jak i specjali-

CIEKAWOSTKA

Z Polski wywodzi się wiele światowej klasy hakerek i hakerów – wymienić można choćby Paulę Januszkiewicz, Joannę Rutkowską, Mateusza Jurczyka, hasherezade, Rafała Wojtczuka czy Michała Zalewskiego. Ponieważ etyczny haking jest bardzo popularny w naszym kraju, na wymienienie wszystkich zabrakłoby miejsca!

Polskie drużyny biorą też udział w zawodach CTF, a dwie z nich – p4 oraz Dragon Sector – od lat zajmują czołowe miejsca w rankingu CTFTime.

3. Celem ataków DoS jest sprawienie, aby dany system komputerowy przestał funkcjonować poprawnie, a więc przestał świadczyć usługi na rzecz swoich użytkowników (stąd nazwa). Ataki DoS często porównywane są do wybryków chuligańskich i nie zawsze są zaliczane do hakingu.

stycznej związanej z bezpieczeństwem komputerowym. Jak więc ćwiczyć (etycznie!) swoje umiejętności, by w przyszłości móc szukać pracy związanej z hakingiem? Opcji jest kilka, ale najlepsza zawsze jest praktyka.

Popularnym pierwszym krokiem zawsze są tzw. *wargame* (pl. dosłownie *gra wojenna*) – czasem nazywane również *hackme* (pl. dosłownie *zhakuj mnie*), czyli serwisy internetowe z praktycznymi ćwiczeniami z różnych działów hakingu oraz rankingiem uczestników. Przykładowym zadaniem może być znalezienie tajnego hasła sprawdzanego przez udostępniony przez twórców skrypt w Pythonie, odszyfrowanie wiadomości zaszyfrowanej algorytmem wymyślonym kilkaset lat temu lub uruchomienie własnego kodu w kontekście strony internetowej stworzonej w PHP i zawierającej intencjonalne błędy.

Listę aktywnych serwisów wargame można znaleźć pod adresem: https://www.wechall.net/active_sites

Po opanowaniu podstaw i przerobieniu znacznej ilości zadań najczęściej kolejnym krokiem są *Capture The Flag* (pl. dosłownie *Zdobądź Flagę*), czyli drużynowe turnieje hakerskie z bardzo podobnymi zadaniami do tych z serwisów wargamingowych. CTFy są obecnie bardzo popularne – w zasadzie co weekend odbywa się gdzieś na świecie kolejny turniej, a większość z nich dopuszcza grę zdalną przez Internet. Warto dodać, że firmy takie jak Google czy Facebook również organizują własne turnieje CTF.

Listę CTFów oraz ogólnoświatowy ranking można znaleźć pod adresem: https://ctftime.org/.

Najczęściej polecanym CTFem dla uczniów szkół średnich jest organizowany przez amerykańską drużynę z Uniwersytetu Carnegie Mellon *picoCTF*, dostępny pod adresem https://picoctf.com/ – zadania z ubiegłych lat często dostępne są również po zakończeniu zawodów.

DRUGA STRONA MEDALU

W obu poprzednich sekcjach skupiłem się na aktywnościach związanych z ofensywną stroną profesjonalnego hakingu – czyli na testach penetracyjnych, przełamywaniu i obchodzeniu zabezpieczeń itp. Należy jednak pamiętać, że równie ważne (a pokusiłbym się o stwierdzenie, że wręcz ważniejsze) role pełnią osoby zajmujące się faktycznym zabezpieczaniem systemów i sieci komputerowych, jak i również specjaliści próbujący wykryć aktywne ataki czy – niczym komputerowi detektywi – prześledzić przebieg włamań, które już miały miejsce (mowa o informatyce śledczej).

Bardzo ważną rolę pełnią tu programistki i programiści. To dzięki ich pracy tworzone są nowe programy, a także rozwijane te już istniejące. Stąd też bardzo ważnym jest, aby osoby, które w przyszłości chcą zawodowo zajmować się programowaniem, w toku swojej edukacji również spędziły trochę czasu, ucząc się podstaw praktycznego hakingu, podstawowych technik, terminów i metod. Naiwnym byłoby sądzić, że jest się w stanie napisać bezpieczną aplikację, nie wiedząc, przed czym tak naprawdę powinniśmy ją zabezpieczyć.

JAK NIE WPAŚĆ W KŁOPOTY

Haking jest ponad wszelką wątpliwość fascynującą dziedziną informatyki! Tym bardziej początkujący etyczni hakerzy muszą pamiętać, gdzie leży granica wyznaczona przez prawo i nigdy jej nie przekraczać. Na zakończenie raz jeszcze przypomnę najważniejsze zasady etycznego hakingu:

- Zawsze należy szanować prywatność innych osób.
- Nigdy nie należy dążyć do wyrządzenia szkody.
- Zawsze należy posiadać zgodę właściciela systemu komputerowego na testowanie jego zabezpieczeń.
- Zawsze należy poinformować właściciela systemu komputerowego o wszystkich znalezionych błędach.
- Zawsze należy trzymać się ściśle wyznaczonych reguł i granic.

Warto zacząć powoli – od nauki programowania, wargame'ów i CTFów. A w razie wątpliwości najlepiej jest zapytać bardziej doświadczone osoby.

Gynvael Coldwind

Etyczny haker. Od 10 lat pracuje w zespole bezpieczeństwa firmy Google.

HTTPS://GYNVAEL.COLDWIND.PL
HTTPS://WWW.YOUTUBE.COM/C/GYNVAELEN

securITum

CYBER AWARENESS

Szkolenia z bezpieczeństwa IT dla pracowników biurowych

WYCIEK DANYCH

SOCJOTECHNIKA

RANSOMWARE

NĘKANIE

WROGIE DZIAŁANIA KONKURENCJI

PRZEJĘCIE DOSTĘPU DO TELEFONU

KRADZIEŻ TOŻSAMOŚCI

CZYSZCZENIE KONTA BANKOWEGO

BEZPIECZNY.SECURITUM.PL

STACJONARNIE

ONLINE

giganci programowania

Kursy programowania dla dzieci i młodzieży

120.000 uczniów

ponad **260** trenerów

12 krajów

Od 7 lat nasze kursy prowadzą zawodowi trenerzy, którzy dzielą się wiedzą i pasją do kodowania.

Tematyka zajęć obejmuje m.in.:

- programowanie gier, programów i aplikacji,
- tworzenie stron internetowych,
- hacking i cyberbezpieczeństwo,
- logiczne i kreatywne myślenie.

KOD: CYBBOOK50

-50zł rabatu na wszystkie kursy dla nowych uczniów

www.gigancіprogramowania.edu.pl