Bezpieczeństwo w sieci

Każdego roku miliony internautów padają ofiarą przestępstw w internecie. Cyberprzestępcy stosują różne zabiegi, aby uzyskać dostęp do naszych kont bankowych, gromadzonych danych oraz sieci kontaktów, których pozyskanie umożliwia im dalsze rozwijanie przestępczej działalności. Wydaje się, że jesteśmy tylko niewinnymi ofiarami tego procederu, jednak wina nierzadko leży także po naszej stronie. Nieprzestrzeganie podstawowych zasad bezpieczeństwa w sieci to jak pozostawianie na noc uchylonych drzwi, albo kluczy w zamku. Z drugiej strony, lekko modyfikując nasze przyzwyczajenia, możemy znacznie utrudnić, a może nawet uniemożliwić przestępcom dostęp do naszych zasobów.

Dzisiaj, w **połowie 2020 r.**, z internetu na świecie korzysta 4,5 mld ludzi. To 60% populacji naszej planety. Połowa ludzkości, czyli prawie 4 mld, korzysta z mediów społecznościowych, a średni światowy czas przebywania w sieci to 6 godzin i 43 minuty dziennie. To prawie 30% doby, 100 dni w roku!

Epidemia SARS-COV-2, która nawiedziła świat z początkiem 2020 r., jeszcze bardziej wzmacnia ten trend. Dzieje się to głównie z powodu konieczności unikania kontaktów bezpośrednich, ale i masowego przekształcania się handlu z formy tradycyjnej w e-commerce oraz wszelkich form rozrywki dostępnych w sieci.

Dane, które nigdy nie śpią!

KLIKNIJ TUTAJ

Kolejnym czynnikiem wpływającym na masowe cyfryzowanie się świata jest **ekspansja urządzeń mobilnych**. Już dzisiaj ponad połowa czasu spędzanego w internecie jest generowana z użyciem smartfonów, które towarzyszą nam w zasadzie wszędzie. Według danych udostępnionych przez **AppAnnie** każde 10 z 11 minut używania smartfonów poświęcamy na korzystanie z aplikacji mobilnych, takich jak komunikatory, media społecznościowe, rozrywka, odtwarzacze wideo, gry, aplikacje zakupowe, bankowe i muzyczne, mapy i nawigacje, jak również aplikacje randkowe. **Firma Ericsson** oszacowała, że użytkownicy internetu na urządzeniach mobilnych zużywają rocznie 500 mld gigabajtów danych, z czego ponad 60% na strumieniowe pobieranie treści wideo, których konsumpcja rośnie w najwyższym dotychczas tempie.

Powyższe dane mogą zaskakiwać, choć wszyscy zdajemy sobie sprawę z faktu, że w momencie czytania tego tekstu są one już nieaktualne – podane wartości rosną bowiem z minuty na minutę. Do ich wzrostu przyczyniają się potężne korporacje i start-upy produkujące i dystrybuujące urządzenia i oprogramowanie, coraz większa dostępność internetu na świecie oraz użytkownicy, czyli każdy z nas, korzystających na co dzień z nieprzebranych zasobów cyfrowego świata.

Śledź na bieżąco cyberataki

TUTAJ i TUTAJ

Najwięksi gracze na wirtualnym rynku, tacy jak Google czy Facebook dostarczają nam masowo usług i aplikacji ułatwiających, a w wielu przypadkach umożliwiających pracę i komunikację. Dostarczają rozrywki oraz ułatwiają dostęp do wiedzy i umożliwiają eksplorowanie i filtrowanie światowych zasobów naukowych. Korzystamy z tych dobrodziejstw chętnie i z wdzięcznością także dlatego, że są one w dużej mierze bezpłatne. Ale czy na pewno? Fakt, za wiele programów i aplikacji nie płacimy ani gotówką, ani bankowym przelewem. Nie oznacza to jednak, że nie płacimy w ogóle. Cyfrowy świat ceni sobie bowiem na równi z pieniądzem, a może nawet bardziej, inną walutę – dane. Dane o nas, które udostępniamy, pobierając „darmowe" oprogramowanie, filmy, gry, surfując w mediach społecznościowych, dokonując zakupów w wirtualnych sklepach. Dane o urządzeniach, których używamy, naszej lokalizacji i sposobie zachowania – w internecie i w świecie rzeczywistym. Informacje o naszym wyglądzie, rodzinie, znajomych, pasjach, aktywnościach, pracy, finansach, marzeniach, zamiarach, etc.

Jeszcze z początkiem XXI wieku sugestia umieszczenia chipu identyfikacyjnego, np. w dowodzie osobistym, spotykała się z oburzeniem i stanowczym sprzeciwem. Była odbierana jako próba nieuprawnionej ingerencji w prywatność i godność osobistą. Dzisiaj własne dane osobowe i wielokrotnie więcej udostępniamy sami i z własnej woli.

Istnieje pozytywny wymiar takiego zachowania. Dzięki gromadzeniu dużych zbiorów danych mogą powstawać, np. takie raporty, jak te cytowane powyżej. Naukowcy z całego świata mogą łączyć siły i nawzajem korzystać z wyników badań oraz niezależnie wypracowanych metod i modeli naukowych.

Poznaj 5 słynnych ataków KLIKNIJ TUTAJ

Big data to niezliczone benefity dla całej ludzkości, ale także ocean możliwości dla cyfrowych piratów. Okazuje się bowiem, że dane, które z taką częstotliwością i w takiej ilości wysyłamy w świat, mogą przysporzyć nam wielu kłopotów, jeśli zostaną skradzione. Przedmiotem ataków mogą być zarówno hasła do stron z bankowością elektroniczną, prywatne zdjęcia czy nawet informacje o logowaniach na konkretne strony internetowe. Przypadki tego typu ataków zdarzają się codziennie, a o skali tego zjawiska mogą świadczyć dane na temat cyberprzestępstw, jakie są stale dokonywane na użytkownikach.

Przyjrzyjmy się tym danym w perspektywie tylko jednego dnia (**stan na maj 2020**), z których wynika, że w ciągu **24 godzin**:

– dochodzi do ok. **62,4 milionów włamań do systemów**,

– średnio **co 39 sekund następuje atak hakerski**,

– wysyłanych jest **6,4 miliarda fałszywych e-maili**,

– ponad **4 739 tysięcy stron jest atakowanych ponad 100 razy**,

– notuje się w samych Stanach Zjednoczonych **ponad 1200 skarg, które dotyczą włamań do komputerów osobistych**.

Z raportów i statystyk dowiadujemy się także, że w poprzednim roku zaledwie w ciągu trzech miesięcy aż 232 292 użytkowników indywidualnych zostało zainfekowanych złośliwym oprogramowaniem (**malware**), w podobnym okresie zanotowano ponad 260 000 skutecznych **ataków phishingowych**, które polegają na podszywaniu się pod osoby i instytucje (np. bankowe). Utrata danych może mieć wiele konsekwencji, zarówno natury społecznej, jak w przypadku utraty wizerunku, jak również ekonomicznej. Warto tutaj wspomnieć chociażby o tym, że w przypadku oszustw typu **ransomware** (blokowanie komputera i żądanie okupu) w ubiegłym roku zgłoszono straty finansowe w wysokości 3,5 biliona dolarów. Czy też o atakach na kryptowaluty, których w samym 2019 roku odnotowano aż 52,7 miliona.

Sprawdź, czy Twoje hasło łatwo złamać:
KLIKNIJ TUTAJ

Dlaczego statystyki notują tak wiele ataków na dane osobowe? Z jednej strony winę za zaistniałą sytuację ponoszą cyberprzestępcy, którzy czyhają na nasze dane i coraz skuteczniej potrafią dokonać włamań do systemów sieciowych. W uzyskiwaniu dostępu do urządzeń użytkowników i kradzieży informacji posługują się oni coraz bardziej precyzyjnymi i innowacyjnymi metodami. Wraz z nieustannym zwiększaniem się skali ataków nie wzrasta jednak świadomość zagrożeń i umiejętność zapobiegania im. Wina nie leży tylko po stronie hakerów, ale także osób, które są celem.

Menedżer na straży Twoich danych:
KLIKNIJ TUTAJ

Brak wiedzy i nierzadko także nieprzestrzeganie podstawowych zasad dotyczących sieciowego bezpieczeństwa powoduje, że umożliwiają one cyberprzestępcom przejęcie danych w łatwy i szybki sposób. Dla przykładu: **63% włamań** do sieci to wynik złamania haseł i nazw użytkowników – wynika to z faktu, że większość haseł składa się z prostej sekwencji znaków. Często nie mamy także świadomości, jak łatwo znaleźć i wykorzystać nasze dane do niepożądanych celów. Informacje o sobie, jakie dobrowolnie udostępniamy w portalach społecznościowych, są jednym z łatwiejszych „łupów" dla hakerów. W samym 2019 roku **zanotowano 849 milionów wycieków danych osobowych** za pośrednictwem tylko jednego z najpopularniejszych serwisów społecznościowych – Facebooka.

Poniżej prezentujemy zbiór zasad świadomego użytkownika internetu. Stosując się do nich, możemy ochronić siebie i swoje dane przed atakami cyberprzestępców.

JAK BEZPIECZNIE KORZYSTAĆ Z INTERNETU?

1. ZAWSZE TWÓRZ SILNE HASŁA.

Hasło zawierające Twoje imię, datę urodzenia, login lub cokolwiek kojarzącego się z Tobą nie jest ani dobre, ani silne. Mocne hasło składa się z małych i dużych liter, liczb, a także znaków specjalnych. Jak zmienić swoje hasło na silniejsze w kilka chwil? Załóżmy, że nasze hasło to „erasmusproject2020" – wystarczy dodać znaki specjalne i duże litery, np. „Er@mu_pro!ect_2020".

2. NIE WYKORZYSTUJ AUTOMATYCZNEGO ZAPAMIĘTYWANIA HASEŁ.

Pamiętaj, że każde konto powinieneś zabezpieczyć innym hasłem – żadnych powtórek. Żadnego automatycznego zapamiętywania. Stworzyłeś silne hasło i boisz się, że je

zapomnisz? Warto użyć programu do przechowywania i zarządzania swoimi danymi do logowań – menedżera haseł. To bezpieczny magazyn, w którym trzymasz wszystkie klucze do swojego cyfrowego życia.

3. ZAWSZE WERYFIKUJ NADAWCĘ WIADOMOŚCI.

Podszywanie się pod zaufanego usługodawcę to częsta praktyka stosowana podczas ataków phishingowych, dlatego zawsze zwracaj uwagę na to, z jakiego adresu przychodzi dany mail, nie otwieraj linków przed ich sprawdzeniem (adres można sprawdzić po naprowadzeniu kursora na dany link). Zwróć uwagę na przestawione litery oraz domenę nadawcy – nadawca podszywający się pod usługodawcę często używa domeny innej niż krajowa lub po prostu zmyślonej.

4. TREŚCI WIADOMOŚCI CZYTAJ ZE ZROZUMIENIEM I NIE DAJ SIĘ PONIEŚĆ EMOCJOM.

Phishing ma to do siebie, że hakerzy próbują grać na emocjach swoich ofiar. Zapamiętaj: Twoja poczta nie zostanie z dnia na dzień dezaktywowana, a Twoje konto w banku czy numer telefonu zablokowane. Jak rozpoznać, że wiadomość jest fałszywa? Zwróć uwagę na poprawność gramatyczną i składniową wiadomości, na przestawione litery, a także na czas na podjęcie działania – cyberprzestępcy często określają wąskie ramy czasowe na podjęcie akcji, podkreślając, że po upływie tego czasu zostaną wyciągnięte konsekwencje (np. blokada konta). Przestępcy nie proponują – żądają.

5. NIE UMIESZCZAJ SKANÓW ANI ZDJĘĆ SWOICH DOKUMENTÓW W SIECI.

Dzięki skanom Twojego dowodu osobistego przestępcy mogą wykraść Twoje dane osobowe i zaciągnąć w Twoim imieniu pożyczkę, którą będziesz spłacał latami.

6. PAMIĘTAJ O USTAWIENIACH PRYWATNOŚCI NA PORTALACH SPOŁECZNOŚCIOWYCH.

Nie ujawniaj wielu prywatnych informacji na portalach społecznościowych, pamiętaj, że wszystko, co raz umieściłeś w sieci, już w niej zostanie. Dwa razy zastanów się nad tym, czy jesteś pewien, że chcesz coś umieścić w internecie.

7. SZYFRUJ DANE.

Jak skutecznie szyfrować dane: KLIKNIJ TUTAJ

Nawet jeśli przestępcy uda się ukraść ważne dla Ciebie dane, są sposoby na to, aby skutecznie uniemożliwić lub przynajmniej utrudnić mu ich odczytanie. Mowa tutaj zarówno o szyfrowaniu sprzętu (dysk, pendrive, inne nośniki danych), plików, jak również poczty elektronicznej.

8. TWÓRZ KOPIE BEZPIECZEŃSTWA.

Jeśli nie chcesz utracić ważnych dla Ciebie informacji, pamiętaj, aby regularnie tworzyć zapasowe kopie danych. Możesz umieścić je na nośnikach zewnętrznych, wewnętrznych, a także na lokacji, z którymi połączysz się za pomocą sieci. O tym, jak możesz to zrobić, przeczytasz tutaj: **https://support.microsoft.com/pl-pl/help/971759/how-to-back-up-or-transfer-your-data-on-a-windows-based-computer**.

9. NIE KORZYSTAJ Z PUBLICZNYCH SIECI WI-FI.

W niezabezpieczonej publicznej sieci bezprzewodowej czeka na Ciebie wiele niebezpieczeństw. Jeśli korzystanie z sieci publicznej jest nieuniknione, pamiętaj o podstawowym zabezpieczeniu. Przede wszystkim: wyłącz udostępnianie swoich danych, unikaj automatycznego łączenia z siecią wi-fi, pobierz VPN (umożliwia to stworzenie sieci

prywatnej przy wykorzystaniu publicznej), włącz wewnętrzny firewall. Szczegółowe wskazówki nt. tego, jak chronić się przed atakami za pośrednictwem publicznej sieci bezprzewodowej, a także informacje o podsłuchach i przechwytywaniu danych przez wi-fi, znajdziesz tutaj: **https://www.binance.vision/pl/security/why-public-wifi-is-insecure**.

10. PRZED ZALOGOWANIEM SIĘ DO BANKU ZAWSZE SZUKAJ ZAMKNIĘTEJ KŁÓDKI.

W lewym rogu w pasku wyszukiwania, klikając w symbol kłódki, możesz wyświetlić informacje o witrynie. Tam sprawdzisz, czy jest ona bezpieczna, czy zawiera certyfikat SSL (odpowiadający za szyfrowanie Twoich danych). Jeśli tak – możesz spać spokojnie, Twoje dane wymieniane z określoną stroną nie wpadną w niepowołane ręce. Ważne, aby kłódka była zamknięta, jeśli jest otwarta – strona nie ma odpowiednich zabezpieczeń.

Sprawdź, czy strona, którą chcesz odwiedzić, jest bezpieczna:
KLIKNIJ TUTAJ

11. NIE POBIERAJ PLIKÓW Z PODEJRZANYCH ŹRÓDEŁ.

Programy w dostępnych darmowych wersjach pobieraj ze stron producenta. Kiedy korzystasz z niezaufanych stron, wraz z aplikacją, którą pobierasz, możesz zainstalować także złośliwe oprogramowanie (malware).

12. DWA RAZY PRZECZYTAJ TO, CO AKCEPTUJESZ W SIECI.

Nieuważne czytanie to pierwszy krok do nieświadomego przekazania swoich danych osobom trzecim, a także do podpisania umowy, której podpisać tak naprawdę nie chcesz. Niesamowita liczba spamu na Twojej poczcie elektronicznej jest spowodowana właśnie bezrefleksyjną akceptacją wszelkich nieobowiązkowych zapisów w regulaminach i zgodach. Pamiętaj, że podczas akceptacji regulaminu serwera czy strony musisz zaznaczyć tylko obligatoryjne zgody. Nieuważne czytanie to także przepustka do pobierania pieniędzy z Twojego konta przez oszustów, którzy wmawiają Ci, że po rejestracji na danej stronie, zagrasz, np. o nowy model iPhone'a.

To tylko 12 prostych zasad bezpiecznego korzystania z zasobów sieci, których bez trudu powinniśmy przestrzegać. A jednak wielu z nich nie przestrzegamy. Któż z nas nie stosuje tego samego hasła do wielu różnych logowań, albo nie korzysta z opcji zapamiętywania haseł? Jak często akceptujemy regulaminy nawet bez ich pobieżnego przejrzenia, byle szybko przejść dalej – pobrać oprogramowanie, zakończyć transakcję czy założyć konto w nowym miejscu? Aby zwiększyć swoje bezpieczeństwo w sieci, konieczna jest zmiana starych, złych nawyków i zastąpienie ich nowymi, dobrymi. Tak o tej zmianie pisze guru rozwoju osobistego i mówca motywacyjny Bryan Tracy:

> *Dobre nawyki są przyczyną Twoich sukcesów i odczuwanego szczęścia i analogicznie złe nawyki są źródłem większości Twoich problemów i zmartwień. Jednak złe nawyki również są wyuczone, dlatego można się ich oduczyć i zastąpić dobrymi*[1].

Zmiana starych nawyków może nie być łatwa, ale korzyści z nowych – bezcenne.

[1] Brian Tracy, 2019: Nawyki warte miliony, Gliwice, s. 20.