DZIEŃ BEZPIECZNEGO INTERNETU

W tym roku **Dzień Bezpiecznego Internetu** przypada na **9 lutego** (wtorek)

Dzień obchodzony jest od 2005 roku, ustanowiony z inicjatywy Komisji Europejskiej. Ma na celu kształtowanie świadomości społecznej dotyczącej niebezpieczeństw, na które narażone są osoby korzystające z Internetu – zwłaszcza dzieci i młodzież. Anonimowość w sieci to powszechny dostęp do cyberprzestrzeni niosącej ze sobą całą gamę zagrożeń. Do najczęściej występujących należą uwodzenie dzieci przez dorosłych o skłonnościach pedofilskich, pornografia oraz cyberprzemoc, czyli publikacja obraźliwych lub kompromitujących materiałów dotyczących innych osób. Wirtualny świat to nie tylko zagrożenia dla dzieci, ale również dla wszystkich uczestników cyberprzestrzeni. Codziennie powstaje grubo ponad 100 tysięcy nowych wirusów. Niektóre z nich to zwykła złośliwość hakerów, inne z kolei mają na celu kradzież cennych informacji, takich jak numery kont czy numery pin. Dotyczy to już nie tylko komputerów, ale również smartfonów i tabletów. Wśród aplikacji najbardziej podatnych na ataki złośliwego oprogramowania znajdują się tak popularne nazwy jak Java, Acrobat Reader czy Adobe Flash. Warto zatem korzystać z dobrego programu antywirusowego.

♦ **Co zrobić aby dostęp do Internetu był bezpieczny:**

- aktualizuj oprogramowanie systemowe (Windows, Linuks, iOS),
- stosuj silne hasła dostępu do systemu oraz sieci domowych,
- nie udostępniaj „sąsiadom” swojej sieci Internet (Wi-Fi).

♦ **Co zrobić, aby korzystanie z Internetu było bezpieczne:**

- aktualizuj oprogramowanie antywirusowe,
- pamiętaj, treści zamieszczone w sieci (zdjęcia, posty, komentarze) nigdy nie zostaną usunięte,
- nie otwieraj załączników w nieznanych wiadomościach e-mail, nieznanych lub budzących wątpliwość co do nadawcy,
- nie udostępniaj w Internecie swoich danych.

Surfując w internecie bądźcie uważni, bowiem istnieje wiele niebezpieczeństw, które mogą przysporzyć Wam kłopotów.

Oto zestawienie 20 najważniejszych zagrożeń.

 Foto:

1. Wirus komputerowy

Znaczenie tego określenia jest bardzo szerokie. Stosujemy je do opisywania klasycznych wirusów, ale również robaków, które potrafią samodzielnie się replikować i rozsyłać poprzez pocztę do naszych kontaktów, a także trojanów, które tworzą w systemie dziury pozwalające przedostać się innym rodzajom zagrożeń. Często o wirusach mówi się w kontekście infekcji poprzez nośniki USB, ale mogą one rozpowszechniać się praktycznie w dowolny sposób - wystarczy plik, do którego mogą się dołączyć, mogą być też częścią większego oprogramowania.

2. Hasło zapamiętane w przeglądarce

Rosnąca liczba serwisów, z których korzystamy, to coraz dłuższa lista haseł i loginów, które musimy zapamiętać. By ułatwić sobie życie, pozwalamy zapamiętywać je przeglądarkom internetowym i korzystamy z funkcji autologowania. Z pozoru praktyczne działanie może poskutkować otwarciem przysłowiowej puszki Pandory, gdy nasz komputer lub smartfon wpadnie w niepowołane ręce.

3. Naruszenie prywatności, stalking

Dbamy o swoja prywatność, o jej nienaruszanie, a jednocześnie często sami wystawiamy ją na forum publiczne. Chwalimy się szczegółami dotyczącymi naszego życia. Takie informacje mogą wykorzystać cyberprzestępcy czy stalkerzy podszywając się pod znajomych i zachęcając nas do wylewności. Również nasze zdjęcia mogą być wykorzystane przez innych użytkowników sieci, by zaszkodzić na przykład naszemu wizerunkowi.

4. Hakerzy

To grupa ludzi o dużej wiedzy na temat komputerów i technik przedostawania się do różnych systemów komputerowych w czasie rzeczywistym. Ich działania manifestują się jako ataki na nasz komputer i wszelkie inne urządzenia, które mają dostęp do sieci (w tym dyski sieciowe, urządzenia mobilne, multimedialne), oraz próby przejęcia nad nimi kontroli.

5. Spam

Teoretycznie niechciana poczta, bo tym jest spam (określany także, jako wiadomości śmieci), powinna być jedynie czynnikiem irytującym. Jednak często w tych pozornie nieszkodliwych treściach kryją się niebezpieczne szkodniki. Cyberwłamywacze liczą, że przez pomyłkę lub z ciekawości otworzymy zainfekowany załącznik, co niestety dość często ma miejsce.

6. Nieodpowiednie treści dla dzieci

Internet pełen jest treści, które nie powinny dotrzeć do maluchów, a zarazem nie są odpowiednio oznaczone. Z kolei ochrona w postaci etykiety "tylko dla dorosłych" czy wymuszenia potwierdzenia wieku jedynie zaciekawi dziecko i wywoła odwrotny do zamierzonego efekt.

7. Pedofilia

Zaburzenie seksualne, które dzięki powszechności internetu stało się wielokrotnie silniejszym zagrożeniem niż przed epoką internetu. Pedofile podejmują działania nawet na powszechnie cenionych stronach i forach. Dzięki anonimowości, jaką daje internet oraz łatwości stworzenia wirtualnej tożsamości, podszywają się oni pod rówieśników lub osoby będące dla młodych użytkowników autorytetami.

8. Bezpieczeństwo danych w sieci

Słowo chmura robi zawrotną karierę, a my coraz chętniej korzystamy z zalet przechowywania w sieci różnorakich danych. Nie tylko zdjęć i filmów, ale również innych tworzonych przez nas treści, niejednokrotnie będących przedmiotem naszej pracy. Korzystanie z usług chmurowych, mimo iż z roku na rok coraz bardziej niezawodne, obarczone jest pewnym ryzykiem, że przechowywane w sieci dane zostaną utracone (na przykład w wyniku awarii pamięci serwera) lub przejęte przez inne osoby.

9. Botnety

To szczególnie nieprzyjemna forma zagrożenia. Dla użytkownika komputera niezauważalna, gdyż oprogramowanie botnetu nie wykonuje działań dla niego szkodliwych (poza ewentualnym wykorzystaniem mocy obliczeniowej i obciążeniem łącza). Grupy zainfekowanych komputerów (zwanych czasem zombie), które tworzą taki botnet, mogą

jednak posłużyć do przestępczej działalności. Obecnie botnety, które były niegdyś dużymi strukturami, stają się coraz mniejsze, a przez to coraz trudniejsze do wykrycia i zablokowania.

10. Fałszywe lajki i ciasteczka

W sieciach społecznościowych często podążamy za nawykami znajomych. To znakomita pożywka dla hakerów, którzy umieszczają na stronach kody wymuszające ich polubienie. My widząc na tablicy, że ktoś znajomy polubił interesujący nas temat, klikamy na link i kłopot gotowy.

Z kolei w przypadku powiadomień o ciasteczkach (cookies) czujemy się zobligowani kliknąć i nawet nie sprawdzamy, czy faktycznie zatwierdzamy politykę ciasteczkową, czy coś całkowicie innego. A może się zdarzyć, że klikając na niewinnie wyglądające powiadomienie, zaakceptujemy niekorzystny dla nas regulamin jakiejś usługi.

11. Fałszywe oprogramowanie ochronne

"Twój komputer jest zainfekowany, skorzystaj z naszego oprogramowania" to jedno z haseł kluczy, które w przypadku naiwnych internautów otwiera drogę cyberprzestępcom do komputerów ofiar. Jednakże i ostrożna osoba może stać się ofiarą, gdy zdecyduje się pobrać z internetu jedną z aplikacji antywirusowych, która jest chwalona przez innych internautów. W rzeczywistości taki fałszywy antywirus jedynie udaje działanie prawdziwego programu. Wyświetla nawet udawane komunikaty o wykryciu i usunięciu wirusów, w tle jednak działając na naszą szkodę.

12. Fałszywe witryny i wyłudzanie danych

tym przypadku najczęściej stosowane jest określenie pharming, czyli podszywanie się pod wrażliwą z perspektywy bezpieczeństwa witrynę, na przykład stronę banku, lub phishing czyli wyłudzanie danych, na przykład poprzez podszywanie się pod znaną osobę lub bazując na ludzkiej empatii. Pharming wykorzystuje techniki oszukiwania systemów DNS, tak, by ruch kierowany był na fałszywe witryny, które choć mają inny adres IP to w przeglądarce identyfikują się takim samym lub bardzo podobnym adresem WWW. Ukrycie fałszerstwa ułatwia podmiana jedynie fragmentu strony, co utrudnia wykrycie adresu złośliwej witryny. Phishing z kolei pozwala osiągnąć podobny efekt, ale w tym przypadku wykorzystywana jest naiwność internauty, od którego bank rzekomo potrzebuje potwierdzenia numeru konta czy danych logowania.

13. Szyfrowanie danych bez naszej wiedzy

Nie chodzi tu o nieumiejętne zablokowanie dostępu do danych na naszym dysku, ale celowe i obliczone na zysk działanie szkodników określanych mianem Cryptolocker. Gdy trafią na

komputer, szyfrują przechowywane na nim dane, od właściciela żądając jednocześnie okupu. Po jego wpłaceniu, najczęściej w bitcoinach, które zapewniają anonimowość odbiorcy wpłaty, jest szansa na otrzymanie klucza deszyfrującego. Jednak tylko szansa, gdyż wpłata, dokonana nawet przed upływem wyznaczonego okresu, nie gwarantuje odblokowania danych.

14. Wykradanie danych osobowych

Informacje o nazwie użytkownika, haśle dostępowym do serwisu sieciowego, a także powiązanych z tymi danymi, numerem konta czy adresem zamieszkania, od strony dostawcy usług przechowywane są teoretycznie w maksymalnie zabezpieczonej formie. Jednakże coraz częściej dochodzi do przejęcia takich baz danych przez cyberprzestępców.

15. Skrócone adresy

Kolejna forma ułatwienia życia w bogatym w treści internecie, którą chętnie wykorzystują przestępcy. Adresy stanowiące skróconą alternatywę dla długich oryginalnych adresów, są łatwiejsze do zapamiętania, zajmują mniej miejsca w korespondencji. Zarazem jednak nie wskazują jednoznacznie, dokąd prowadzą, a często kierują do szkodliwej witryny.

16. Literówki w adresach WWW

Wpisując szybko adres strony na klawiaturze nietrudno o pomyłkę, przestawienie liter lub zapomnienie o wpisaniu danego znaku. I choć szanujący się operatorzy witryn sieciowych dbają o rejestrację podobnie brzmiących adresów, nie jest to regułą. Zresztą liczba alternatyw jest tak duża, że trudno przewidzieć jak pomyli się internauta. Otworzenie witryny o podobnie brzmiącej nazwie czasem prowadzi do nic nieznaczącej strony z reklamami, ale czasem może kompletnie zablokować komputer.

17. Otwarte sieci Wi-Fi

Niebezpieczne są na dwa sposoby. W pierwszym przypadku dotyczy to konfigurowanych przez nas domowych sieci, które nie są w żaden sposób zabezpieczone i dają dostęp niepowołanym osobom nie tylko do internetu, ale także do naszych danych. Drugi scenariusz to korzystanie przez nas z otwartych sieci Wi-Fi, o których kompletnie nic nie wiemy. Choć tworzenie takich sieci ma służyć ułatwieniu dostępu do internetu, często taka droga na skróty może być opłakana w skutkach, gdyż kompletnie nie wiemy, kto kontroluje przepływ danych przez taki punkt dostępowy.

18. Ataki ukierunkowane

Jest to ogólne określenie ataku, który wykorzystuje ludzkie przyzwyczajenia i podatność na błędy w pozornie trywialnych sytuacjach. Cybeprzestępcy mogą tak spreparować szkodniki komputerowe, by zmaksymalizować szanse ich uruchomienia. Istotna w tym przypadku jest bardziej znajomość atakowanego i socjotechnika niż wyrafinowanie zastosowanego oprogramowania.

19. Niezaktualizowane oprogramowanie

Wysoki stopień skomplikowania oprogramowania instalowanego na komputerach i innych urządzeniach sprawia, że łatwiej o zaistnienie słabych punktów, czyli dziur. Jeśli nie zostaną one usunięte, na przykład poprzez aktualizację lub nową wersję programu, mogą być wykorzystane przez cyberprzestępców. Dotyczy to nie tylko systemu operacyjnego, ale również wszelkich aplikacji użytkowych, a przede wszystkim pakietów zabezpieczających.

20. Nadmierna wiara w odporność na zagrożenia

Przekonanie, że doskonale potrafimy sobie poradzić z każdym zagrożeniem, może uśpić naszą czujność. Często nie zdajemy sobie sprawy z różnorodności technik cyberprzestępczych. Wiara we własne umiejętności sprawia, że ignorujemy rzeczywiste sygnały o zagrożeniu.

Jeśli chcesz wiedzieć więcej, jak ochronić siebie, wejdź na: www.bezpieczenstwo.onet.pl

Dlatego jednym z najlepszych narzędzi zabezpieczających nasze urządzenia, dane oraz prywatność jest zdrowy rozsądek. Jeśli nie będziemy uważać, w jakie linki klikamy, jakie otwieramy załączniki, to na własne życzenie możemy napytać sobie biedy. Oczywiście zainstalowanie pakietu ochronnego jest bardzo dobrym pomysłem, ale jego używanie nie zwalnia nas z ostrożności.

- **Bitdefender Internet Security**
- **Kaspersky Internet Security**
- **McAfee Internet Security**
- **Norton Security**

Bezpiecznego surfowania.

Pozdrawiam ☺ Barbara Magalska