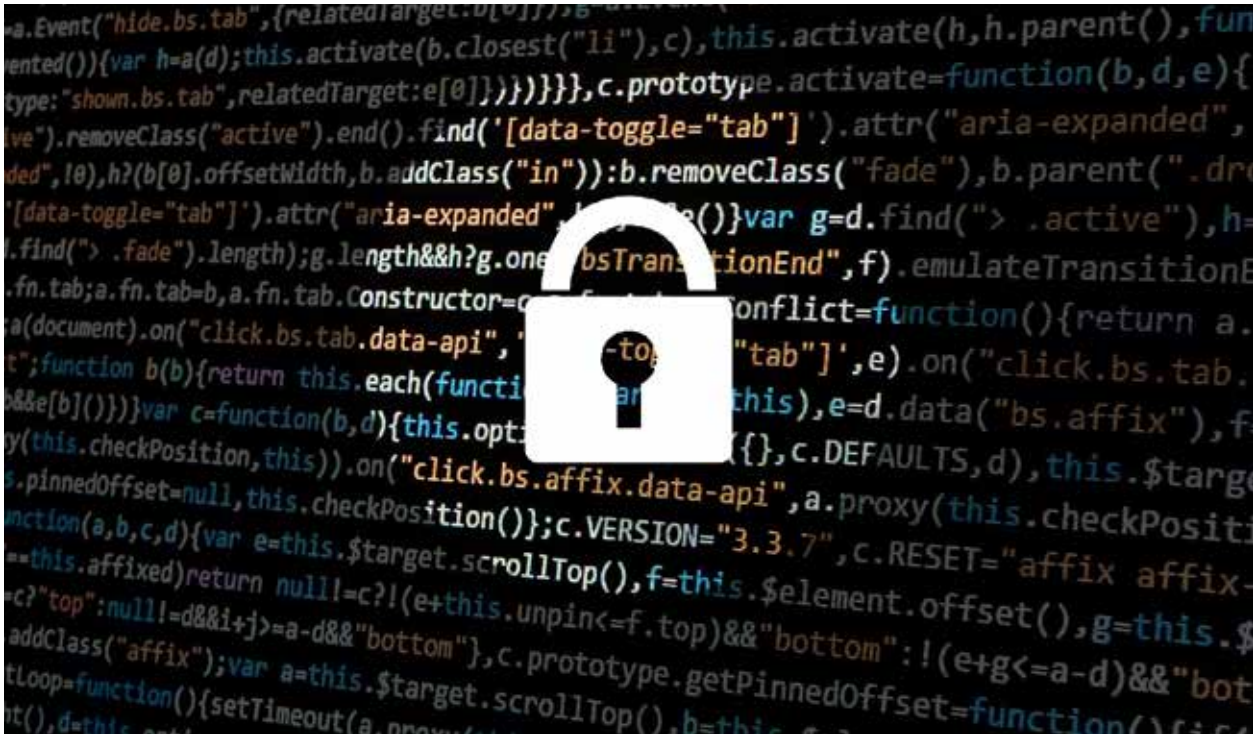
Tadeusz Szulc, Ekspert IT, Członek Rady Programowej Wydawnictwa „Nowa Energia"

Wzmacniaj swoje bezpieczeństwo informatyczne

Zwykło się twierdzić, że bezpieczeństwo informatyczne jest jak pogoda, w końcu… zawsze jakaś jest. Czasami o takiej charakterystyce, jak pies Azor z felietonu Stefana Wiecheckiego.



fot. Pixabay.com

Bohater felietonu Wiecha wybrał się ze swoim psem na szczepienia przeciwko wściekliźnie.

- Rasowy?
- Poczwórnie.
- To znaczy, że jak?
- Znaczy nogi jamnika, morda buldoga, uszy wyżła, ogon owczarka - a razem, uważasz pan, mój pies.

O ile pies Azor sprawia na czytelniku przyjemne wrażenie i wzbudza powszechną sympatię, o tyle system informatyczny zabezpieczony przypadkowo dobranymi rozwiązaniami nie gwarantuje, że wprowadzone dane nie zostaną utracone, nie ulegną zniekształceniu i nie zostaną pozyskane przez nikogo nieuprawnionego.

Prawda jednak jest taka:

- 30 kwietnia br. poinformowano, że policja i prokuratura rozbiły międzynarodowy gang zajmujący się kradzieżami pieniędzy z kont bankowych metodą tzw. phishingu.

W działalność grupy zaangażowanych było około 500 osób, ukradli łącznie ponad 154 mln zł. Według ustaleń prokuratury grupa działała co najmniej od czerwca 2011 r. do kwietnia 2016 r. na terenie kilkunastu krajów Unii Europejskiej oraz Ukrainy i Rosji. Jej członkami byli głównie Polacy i Łotysze, a poszkodowanymi - osoby fizyczne, firmy i instytucje z krajów europejskich.

- 24 kwietnia br. na szeregu stron internetowych pojawiła się informacja, że zaatakowano i zaszyfrowano stronę internetową Ministerstwa Energetyki i Przemysłu Węglowego Ukrainy.

Za jej odblokowanie sprawcy zażądali okupu w wysokości 0,1 bitcoina (około 900 dolarów).

- W połowie kwietnia br. brytyjski dziennik „Guardian", omawiając badania naukowców z Yale University i francuskiej organizacji Exodus Privacy, upublicznił informację, że trzy na cztery aplikacje na Androida zawierają co najmniej jeden skrypt śledzący - tzw. tracker.

To dzięki tym śledzącym nas skryptom korporacje gromadzą wiedzę nie tylko o oglądanych przez nas stronach internetowych czy zakupach. Potrafią również ustalić, gdzie, kiedy i z kim przebywamy.

- 20 marca br. odkryto, że kolejny raz zaatakowane zostały polskie banki.

W sklepie Google Play umieszczona została aplikacja „Bankowość uniwersalna Polska", która agregowała formularze logowania do 21 polskich banków. Z jej poziomu nieświadomi użytkownicy, podając swoje prawdziwe loginy oraz hasła, mogli sądzić, że logują się do swoich rachunków. Aplikacja została tak skonstruowana, by służyła do kradzieży danych logowania do rachunków bankowych, a następnie do wyprowadzania z nich pieniędzy.

- Również w marcu br. zaatakowano serwery Teatru Współczesnego w Warszawie.

Nieznani sprawcy przejęli (a Teatr utracił) tzw. plany widowni na spektakle grane od 21 marca aż do 6 maja br. W tym okresie w programie Teatru było około 30 przedstawień, każde na trzysta osób.

- 10 listopada 2017 została zaatakowana strona internetowa lotniska w Modlinie.

Przez pewien czas na stronie internetowej portu pojawiał się wizerunek uśmiechniętego diabła a w tle słychać było muzykę.

Wszystkie te fakty są poważnym, niepokojącym zagrożeniem informatycznej wizji naszej przyszłości i mogą odwrócić naszą skalę wartości, a przecież nadchodące zmiany to rezultat długookresowych tendencji, których oddziaływanie na nasz świat już się rozpoczęło. Czy mamy całkowicie zrezygnować ze zrewolucjonizowania tego jak pracujemy, jak uczymy się, jak kupujemy, jak spędzamy czas wolny czy komunikujemy się ze sobą?

Oczywiście, najbardziej przezorni mają zawsze arsenał skutecznych narzędzi zabezpieczających pochodzących z różnych dyscyplin. Przegrywają za to ci, którzy ograniczają się do niewielu metod albo mają przestarzałe narzędzia. Przetrwają ci, którzy czerpią z wielu szkół. Nieodżałowany profesor Jerzy Vetulani twierdził, że „mądry nauczy się od każdego".

Choć liczba obserwowanych ataków nie rośnie w zastraszającym tempie to jednak zmieniają się ich cele, a metody stają się coraz bardziej wyrafinowane. Coraz częściej cierpią na nich urządzenia Internetu Rzeczy. Polityka bezpieczeństwa informatycznego - jak każda forma zarządzania - musi zmieniać się wraz ze zmianą otoczenia, w którym funkcjonuje, bo system gospodarczy jest w ciągłym ruchu. W ramach tej polityki obowiązkowo należy prowadzić analizy czy nie powstaje rozbieżność między aspiracjami (wizerunek pożądany), a rzeczywistością (wizerunek rzeczywisty) poziomu bezpieczeństwa. Ustalenie poziomu tej rozbieżności stanowi punkt wyjścia do formułowania strategii, celów i działań naprawczych, zmierzających do minimalizacji luki między nimi.

Jeżeli różnica ta będzie znacząca, to pozom bezpieczeństwa informatycznego będzie odpowiadał poziomowi aktywności strażaków z felietonu Wiecha, którzy „gasili tylko na parterze, bo po drabinach doktorzy jem zabronili chodzić z powodu otłuszczenia serca".

Do wzrostu zagrożenia informatycznego przyczynił się także rozwój samej … informatyki: rozrosła się, rozgałęziła i wyspecjalizowała. Zaszedł tutaj proces podobny jak w przypadku innych nauk ścisłych: ilość i różnorodność wiedzy w każdej ze składowych jest tak olbrzymia, że nikt nie jest w stanie ogarnąć całości.

Niemal każdy fragment naszego życia staje się usieciowiony i dostępny w „chmurze". To niesie ze sobą ogromne konsekwencje.

Epoka swobód i praw obywatelskich przeżywa na Zachodzie kryzys, a niezbywalność praw jednostki do wolności czy prywatności okazuje się coraz mniej znaczyć. Coraz częściej godzimy się na inwigilację i używając smartfona z góry zakładamy, że każdą naszą czynność śledzą niewidzialni szpiedzy.

Doskonalone, w celach komercyjnych, technologie trafiają również do struktur, które zniewalają ludzi podejrzeniami, obawami i błędnymi skojarzeniami. Istnieje pokusa pokonania demokratycznych mechanizmów i ich obejścia drogą szybkich manewrów stosujących informatyczną przemoc w nieprzewidywalnej i zaskakującej nas formie. Stosuje się w tym celu np. techniki budowania przesądów, techniki uzależniania innych od siebie, techniki tworzenia autorytetu, któremu nie spo-

sób się oprzeć, techniki zakotwiczania (ściągania czyichś myśli w określony obszar) czy techniki kierowania wrażeniem.

Do zapobiegania inwigilacji (nas i firm w których pracujemy) są służby. To one powinny przeprowadzać szeroko i kompleksowo czynności diagnozowania oraz prognozowania zagrożeń i zachowań podmiotów. Ale nawet posiadanie kilku różnych agencji nie daje żadnych gwarancji, bowiem coraz częściej uczestniczą one w różnego rodzaju grach rynkowych. Co ciekawe, o ile amerykańskie agencje bezpieczeństwa oskarżają chińskie firmy (Huawei i ZTE) o instalowanie w produktach tzw. tylnych drzwi (backdoor) zapewniających władzom w Pekinie dostęp do wrażliwych informacji np. o miejscu pobytu użytkownika, o tyle niemieckie, planują stworzenie regulacji prawnych, które będą zmuszać producentów sprzętu elektronicznego do wbudowywania tylnych drzwi w urządzenia (mają one umożliwiać organom ścigania i służbom łatwiejszy dostęp do danych).

Sprawa backdoor'a - na dzień dzisiejszy - jest co najmniej ambiwalentna. Jest cała grupa ekspertów, którzy uważają, że tworzenie backdoora jest bardzo niebezpieczne (wręcz nieodpowiedzialne), nawet jeżeli jego pierwotne zastosowanie, takie jak walka z cyberprzestępczością, jest jak najbardziej słuszna. Co ciekawe firmą, która zdecydowała się na „tylne drzwi" jest sam amerykański … Microsoft (!). Microsoft'owy backdoor został opracowany dla mechanizmu Secure Boot i dzięki niemu może przeprowadzać wewnętrzne testy. W zamyśle przedstawicieli Microsoftu ma to być dodatkowa ochrona przed … hakerami. Również koreański Samsung w kilku swoich urządzeniach w fabrycznych kompilacjach Androida stosuje backdoor'a i … daje dostęp do danych osobistych użytkownika (oraz możliwość ich modyfikowania) każdemu, kto będzie chciał to wykorzystać.

Zarówno w USA jak i w Niemczech bardzo mocno lobbuje się za wprowadzenia prawa dotyczącego możliwości zdalnego hakowania (dostępu do zasobów) dowolnego komputera. Oczywiście, aktywiści na rzecz prywatności wskazują na zagrożenia związane z nowymi propozycjami prawnymi. Ich zdaniem, taka regulacja prawna pozwoli uzyskać kontrolę nad całością ruchu internetowego, a także mieć wgląd w komunikację wszystkich użytkowników internetu.

Szereg światowych ekspertów zajmujących się bezpieczeństwem informatycznym twierdzi, że „sprzęt jest kluczem do bezpieczeństwa informacji". Wynika to z faktu, że sieci są nośnikami informacji o różnym stopniu wrażliwości. Muszą być zatem chronione na kilku poziomach. Na poziomie technicznym czyste oprogramowanie nie wystarcza. Potrzebny jest także zaufany komponent sprzętowy.

Warto zapoznać się z opiniami tych ekspertów. Większość z nich wybiera się do Norymbergi, aby wziąć udział w największych europejskich targach bezpieczeństwa IT (od 9 do 11 października 2018). Warto nadmienić, że jest to jedno z trzech najważniejszych wydarzeń związanych z bezpieczeństwem cybernetycznym na świecie gromadzące, między innymi, oficerów bezpieczeństwa, menedżerów centrów komputerowych, administratorów sieci, dyrektorów technologicznych i decydentów zarządzania. Więcej informacji o targach na https://www.it-sa.de/en/become-exhibitor.

„Dziś głównym zasobem gospodarczym jest wiedza" mówi jeden z najważniejszych myślicieli XXI w., światowej sławy izraelski historyk i filozof Yuval Noah Harari (profesor Uniwersytetu Hebrajskiego w Jerozolimie).

We współczesnej gospodarce o sukcesie rynkowym przedsiębiorstwa często przesądza wiedza zgromadzona przez jego pracowników oraz zawarta w danych przez nie gromadzonych.

Szukajmy tej wiedzy!

Jedno jest pewne: hakerzy jej szukają i działają na różne sposoby, z rozmysłem, z uwagą i premedytacją odnosząc sukcesy nawet w przypadku sieci, w których wdrożono złożone i kosztowne zabezpieczenia.

Przyczyn hakerskich ataków jest wiele: chęci wzbogacenia się, złośliwa potrzeba destrukcji czy pokusa przejęcia kontroli i płynące z niej poczucie władzy.

Często stosowane przez hakerów metody cyberataków to:

- wysyłanie zainfekowanych informacji i podszywanie się pod użytkownika sieci *(spoofing)*;
- udawanie osoby lub instytucji godnej zaufania i wyłudzanie danych lub pieniędzy *(phishing)*;
- tworzenie imitacji strony internetowej, np. banku i uzyskanie danych logowania *(pharming)*;
- po włamaniu się do sieci, monitorowanie przepływu danych, takich jak nazwy użytkowników czy hasła *(sniffing)*;
- spowodowanie blokady sieci przez zajęcie wszystkich wolnych zasobów serwerów, połączone z równoczesnym atakowaniem ich z wielu komputerów *(DDoS)* albo wysyłaniem ogromnych ilości danych, co obciąża serwer *(SYN flooding)*.

Tajemnicą poliszynela jest fakt zatrudniania przez rządy wielu krajów armii hakerów do szpiegowania i wykradania tajnych danych. To bardzo zróżnicowana grupa fachowców o interdyscyplinarnej wiedzy potrafiąca ingerować i wykradać dane z sieci, nie ujawniając swojej działalności. Ich praca polega również na wymyślaniu nowych metod ataku i z niej są rozliczani. Najczęściej pracują w centre of excellence. Od lat toczą oni wojny, których nikt nie chce nazwać wojną. Tu nikt nie mówi o przestrzeganiu jakichkolwiek standardów.

□