



◀ Nr: 23/04

Aktualne wydanie

- [POLSKA](#)
- [ŚWIAT](#)
- [BIZNES](#)
- [NAUKA](#)
- [SPOŁECZEŃSTWO](#)
- [KULTURA](#)
- [PERYSKOP](#)
- [STAŁE RUBRYKI](#)
- Online**
- [Archiwum](#)
- [Dodatki specjalne](#)
- [Wydania specjalne](#)
- [Rankingi](#)
- [Wyniki sond](#)
- [Newsreportaż](#)
- [Wyszukiwarka](#)
- [Czat](#)
- [Podporusz 2004](#)
- [Ankieta](#)

Forum

- [Spór o kamienice](#)
- [Użytkownicy](#)
- [Opinie](#)
- [Dyskusje](#)
- [Złapani na pracę](#)

Sklepik online

[Koszyk](#)

Newsweek

POLSKA

poniedziałek, 31 maja 2004 r.

Newsweek Polska | Strona główna ▶ Archiwum

NAUKA

Newsweek numer 08/01, strona 72.

Czekając na atak

Technologie

Najważniejsze systemy informatyczne w Stanach Zjednoczonych mają mnóstwo słabych punktów. Teraz one mogą stać się łatwym celem ataków terrorystycznych.

Mówisz: "terroryzm" - myślisz: "samoloty". A może powinniśmy pomyśleć o zamachu na sieć energetyczną Stanów Zjednoczonych? Wiosną tego roku ktoś włamał się do sieci komputerowej firmy California Independent System Operator (Cal-ISO), zarządzającej przesyłaniem energii elektrycznej na duże odległości. Specjaliści z Cal-ISO mówią jednak, że rzeczywisty cel ataku stanowił testowy system komputerowy, który nie był połączony z główną siecią. Choć w tym wypadku nie dokonano żadnych zniszczeń, to w świetle wydarzeń z 11 września problem włamań do sieci informatycznych spędza sen z powiek szefom tej firmy. - Jesteśmy bardziej czujni i widzimy teraz potrzebę wprowadzenia dodatkowych środków bezpieczeństwa - mówi Gregg Fishman, rzecznik prasowy Cal-ISO.

Przed zagrożeniem cyberterroryzmem, które może dotyczyć każdej firmy stoi, także Cal-ISO. Dotychczas terrorystyczne ataki na systemy elektroniczne były nieliczne, a ataki internetowe przeprowadzały pojedyncze osoby. To samo można było powiedzieć o umieszczaniu wirusów w Internecie. - Najwyraźniejszym przejawem cyberterroryzmu w ostatnich latach była niewielka wojna między amerykańskimi i chińskimi hakerami. Niszczili sobie nawzajem witryny internetowe - mówi Fred Rica z firmy doradczej Pricewaterhouse Coopers, specjalista od oceny zagrożeń. Tak było do niedawna. Dziś wielu ekspertów obawia się, że czas stosunkowo nieszkodliwych działań w cyberprzestrzeni może się wkrótce skończyć.

Służby miejskie, telekomunikacja i fabryki, które zawsze były narażone na ataki terrorystyczne, obecnie stanowią wymarzony cel ataków elektronicznych. Operatorzy sieci sterują ważnymi systemami na odległość. Nawet jeżeli systemy te nie są podłączone do Internetu, to opierają się na łączności telefonicznej. Niewątpliwie jest to bardzo wygodne z uwagi na wielkie przestrzenie między poszczególnymi obiektami, ale niezbyt bezpieczne. George Kurtz, autor książki "Hacking Exposed" ("Obnażeni hakerzy") i konsultant firmy Foundstone Inc, twierdzi, że osoba ze zmysłem technicznym ma 90 procent szans na włamanie się do takiego systemu. Natomiast zatrzymanie jej jest bardzo trudne. Włamania można dokonać właściwie z każdego miejsca kuli ziemskiej.

Strona: 1/4 Dalej >>

Wybierz stronę: **1** | 2 | 3 | 4

Erik Sherman

Artykuł ukazał się w tygodniku Newsweek Polska, w numerze 08/01 na stronie 72

Rekor
Kliknij,
tę stro

Z
z
lep
Ne

S
OK



◀ Nr: 23/04

Aktualne wydanie

- [POLSKA](#)
- [ŚWIAT](#)
- [BIZNES](#)
- [NAUKA](#)
- [SPOŁECZEŃSTWO](#)
- [KULTURA](#)
- [PERYSKOP](#)
- [STAŁE RUBRYKI](#)
- Online**
- [Archiwum](#)
- [Dodatki specjalne](#)
- [Wydania specjalne](#)
- [Rankingi](#)
- [Wyniki sond](#)
- [Newsreportaż](#)
- [Wyszukiwarka](#)
- [Czat](#)
- [Podporusz 2004](#)
- [Ankieta](#)

Forum

- [Spór o kamienice](#)
- [Użytkownicy](#)
- [Opinie](#)
- [Dyskusje](#)
- [Złapani na pracę](#)
- Sklepik online**
- [Koszyk](#)

Newsweek

POLSKA

poniedziałek, 31 maja 2004 r.

Newsweek Polska | Strona główna ▶ [Archiwum](#)

NAUKA

Newsweek numer 08/01, strona 72.

Czekając na atak Technologie

Najważniejsze systemy informatyczne w Stanach Zjednoczonych mają mnóstwo słabych punktów. Teraz one mogą stać się łatwym celem ataków terrorystycznych.

Zagrożony atakiem jest także system transportowy. Przedsmak tego, co może się zdarzyć w przypadku ataku elektronicznego, dała nam historia pewnego nastolatka, który w 1997 roku zdołał połączyć się z centralą telefoniczną lotniska w Worcester, w stanie Massachusetts, i zupełnie przypadkowo przerwał łączność wieży kontrolnej na sześć godzin. Kontrolerzy ruchu lotniczego musieli naprowadzać samoloty przy użyciu telefonów komórkowych i radiostacji zasilanych z akumulatorów.

W zeszłym roku Główny Urząd Księgowości wydał raport stwierdzający, że program bezpieczeństwa komputerowego Federalnego Urzędu ds. Lotnictwa zawiera "dużo słabych punktów". Chodziło o nieprzetestowane systemy kierowania ruchem lotniczym, a także o ignorowanie przez lotniska obowiązku stosowania kodów dostępu i usuwania usterek w oprogramowaniu systemów bezpieczeństwa.

Wiele firm jest znacznie bardziej narażonych na ataki elektroniczne, niż im się wydaje. - O przeważającej większości cyberataków nic nie wiemy, gdyż nawet ich ofiary nie zdają sobie sprawy z tego, że zostały zaatakowane - mówi Amit Yoran, prezes Riptech Inc., firmy świadczącej usługi w zakresie bezpieczeństwa. Yoran jest także byłym dyrektorem programu bezpieczeństwa informatycznego w Departamencie Obrony. - Niektóre prowadzone przez nas badania wykazały, że spośród wszystkich osób, do których włamał się w czasie prób, mniej niż trzy procent wykryło atak lub nań zareagowało.

Łatwym celem stają się niektóre witryny internetowe. - Nie możesz zostać zaatakowany, jeżeli nie jesteś w sieci - mówi Elad Baron, dyrektor generalny firmy Whale Communiation z Fort Lee w stanie New Jersey, która sprzedaje systemy zwiększające bezpieczeństwo. - Kiedyś wszystkie kluczowe sieci były fizycznie odłączone od Internetu. Ale raz po raz dzieje się coś zaskakującego. Oczywiście oficjalnie firma może nie być podłączona do Internetu, ale zawsze znajdzie się jakiś specjalista, który musi mieć dostęp do firmowych plików z domu, a sam ma internetowe łącze.

<< Wstecz **Strona:** 2/4 Dalej >>

Wybierz stronę: 1 | **2** | 3 | 4

Erik Sherman

Artykuł ukazał się w tygodniku Newsweek Polska, w numerze 08/01 na stronie 72

[koszyk](#) [Dodaj wydanie do koszyka](#)

Forum | Weź udział w jednej z poniższych dyskusji

Rekor
Kliknij,
tę stro

Z
z
lep
Ne

S
OK



◀ Nr: 23/04

Aktualne wydanie

POLSKA

ŚWIAT

BIZNES

NAUKA

SPOŁECZEŃSTWO

KULTURA

PERYSKOP

STAŁE RUBRYKI

Online

Archiwum

Dodatki specjalne

Wydania specjalne

Rankingi

Wyniki sond

Newsreportaż

Wyszukiwarka

Czat

Podporusz 2004

Ankieta

Forum

Spór o kamienice

Użytkownicy

Opinie

Dyskusje

Złapani na pracę

Sklepik online

Koszyk

Newsweek

POLSKA

poniedziałek, 31 maja 2004 r.

Newsweek Polska | Strona główna ▶ Archiwum

NAUKA

Newsweek numer 08/01, strona 72.

Czekając na atak

Technologie

Najważniejsze systemy informatyczne w Stanach Zjednoczonych mają mnóstwo słabych punktów. Teraz one mogą stać się łatwym celem ataków terrorystycznych.

Bezpieczeństwo elektroniczne staje się coraz ważniejsze, gdyż nie można po prostu zamknąć wszystkich dróg dostępu elektronicznego do Stanów Zjednoczonych. Biorąc pod uwagę sposób, w jaki tworzone są systemy informatyczne i jak pisane są programy komputerowe, należy liczyć się z istnieniem miejsc dostępu do sieci nieznanymi nawet kierownictwu danej firmy. Punkty te są jak nielegalne przejścia graniczne. - Łatwo jest je zaatakować z dowolnego miejsca. Nie da się odciąć dostępu do Internetu ludziom na całym świecie - mówi Elad Baron.

Niektóre prywatne firmy są jeszcze bardziej nieostrożne, jeśli chodzi o informacje dotyczące ich systemów komputerowych. Część danych rozpowszechniana jest w materiałach dostarczanych przez przedstawicieli handlowych. - Bardzo często potrzebne informacje można znaleźć w fachowych pismach publikowanych przez firmy komputerowe - mówi John Woodward, dyrektor czuwający nad bezpieczeństwem systemów informatycznych w firmie MITRE, świadczącej usługi doradcze w dziedzinie bezpieczeństwa. Firma ta pracuje dla niektórych agend rządu federalnego - między innymi dla Pentagonu.

Richard B. Isaacs, dyplomowany specjalista ds. ochrony i wiceprezes Lubrinco Group, firmy świadczącej usługi w zakresie prowadzenia dochodzeń i ochrony, mówi jak, wyglądała do niedawna witryna Departamentu Obrony. - W jednym miejscu umieszczono zdjęcie bazy wojskowej. Jeżeli przesuwano się po nim kursor, to automatycznie uzyskiwało się długość i szerokość geograficzną danego miejsca - wspomina Isaacs. - Dlaczego Departament Obrony udostępnił wszystkim swoją witrynę? Co więcej, dopiero pod koniec września tego roku Narodowa Agencja Kartograficzna wstrzymała sprzedaż szczegółowych map z obiektami wojskowymi.

Niektórzy eksperci uważają jednak, że terroryści nie będą koncentrować się na atakach elektronicznych.

- Zajmując się problemem terroryzmu od 30 lat, zorientowałam się, że terroryści wolą, aby zniszczenia, jakich dokonują, były widoczne - mówi Martha Crenshaw, profesor uniwersytetu Wesleyan w Middletown w stanie Connecticut, autorytet w sprawach terroryzmu. - Jeżeli będą mieli do wyboru atak przy użyciu materiałów wybuchowych lub sprzętu elektronicznego, to wybiorą - jak sądzę

<< Wstecz **Strona:** 3/4 Dalej >>

Wybierz stronę: 1 | 2 | **3** | 4

Erik Sherman

Rekor
Kliknij,
tę stro

Z
z
lep
Ne

S
OK



◀ Nr: 23/04

Aktualne wydanie

POLSKA

ŚWIAT

BIZNES

NAUKA

SPOŁECZEŃSTWO

KULTURA

PERYSKOP

STAŁE RUBRYKI

Online

Archiwum

Dodatki specjalne

Wydania specjalne

Rankingi

Wyniki sond

Newsreportaż

Wyszukiwarka

Czat

Podporusz 2004

Ankieta

Forum

Spór o kamienie

Użytkownicy

Opinie

Dyskusje

Złapani na pracę

Sklepik online

Koszyk

Prenumerata

Newsweek

POLSKA

poniedziałek, 31 maja 2004 r.

Newsweek Polska | Strona główna ▶ Archiwum

NAUKA

Newsweek numer 08/01, strona 72.

Czekając na atak

Technologie

Najważniejsze systemy informatyczne w Stanach Zjednoczonych mają mnóstwo słabych punktów. Teraz one mogą stać się łatwym celem ataków terrorystycznych.

- wybuch.

Zabezpieczenie infrastruktury nie jest zadaniem niemożliwym. - Lista miejsc, które trzeba chronić, nie jest nieskończona. Znajdują się na niej zakłady usług komunalnych, sieć energetyczna i gazowa, elektrownie jądrowe i budynki wojskowe - mówi Elad Baron. Najpopularniejsze sposoby na uniknięcie zagrożenia to zrezygnowanie z komunikacji przy użyciu łącz telefonicznych, odłączenie systemów od Internetu i zainstalowanie programów wykrywających intruzów. Jednak wprowadzanie nowych środków bezpieczeństwa będzie wymagało woli politycznej i pieniędzy.

Przez lata sektor prywatny ignorował ostrzeżenia dotyczące bezpieczeństwa systemów komputerowych. Teraz jednak gotowy jest do współpracy. - Bezpieczeństwo nie jest już traktowane po macoszemu - mówi George Kurtz. - Rozmawiałem z jednym z klientów, który powiedział, że wszystko, co zawiera teraz słowo "bezpieczeństwo", zostanie zaakceptowane.

Czy jednak władze nie posuną się za daleko? Według Shari Steele, dyrektora wykonawczego Electronic Frontier Foundation, ich propozycje idą stanowczo za daleko. - Być może schwytyją w swoją sieć terrorystów, ale złapią także innych ludzi. Steele podaje przykład podatnika, w geście protestu uszkadzającego stronę internetową urzędu skarbowego. Nowe prawo uznałoby to za akt terroryzmu przeciwko władzom federalnym. - Jest to przestępstwo o charakterze kryminalnym, za które człowiek powinien zostać skazany, ale nie jest to terrorizm. Musimy bardzo uważać, zwłaszcza że kary za terrorizm mogą być bardzo wysokie.

Mick Jagger powiedział kiedyś: "Nie zawsze można mieć to, co się chce. Czasem jednak, gdy dostaniemy to, czego chcieliśmy, może się okazać, że mamy więcej niż trzeba".

<< Wstecz **Strona:** 4/4

Wybierz stronę: 1 | 2 | 3 | 4

Erik Sherman

Artykuł ukazał się w tygodniku Newsweek Polska, w numerze 08/01 na stronie 72

koszyk Dodaj wydanie do koszyka

Forum | Weź udział w jednej z poniższych dyskusji

Dobre i złe strony elektrowni jądrowych (odpowiedzi: 2)

Autor: Evi

Data: 18.02.2004 10:54

Forum | Rozpocznij nową dyskusję

Rekor
Kliknij,
tę stro

Z
Z
lep
Ne

S
OK