Cyberprzestrzeń i prawo

Cyberprzestrzeń jest dziś jedną z wielkich granic prawnych. Stein Schjolber

Wprowadzenie

Gdy tylko cyberprzestrzeń i handel elektroniczny powstały w połowie lat 90., cyberprzestępczość rozkwitła równolegle. Cyberprzestępczość podwaja się każdego roku pod względem liczby incydentów, a także strat pieniężnych. Niemożliwe jest określenie ilościowe cyberprzestępczości, ponieważ większość ofiar widzi dalsze straty w reklamowaniu swojej niezdolności do obrony przed tym współczesnym zagrożeniem. Ciekawe jest to, że spośród złapanych cyberprzestępców zdecydowana większość przyznała się do winy. Wynika to z faktu, że zebrane fakty - zapisy ruchu sieciowego - powodują hermetyczne przypadki. Jeśli chodzi o upowszechnianie przepisów dotyczących walki z cyberprzestępczością, „tekst będzie musiał zachować pewną elastyczność, pozwalając na względnie zmienny charakter różnych form cyberprzestępczości i szybkość, z jaką rozwijają się nowe technologie". Wszelkie traktaty międzynarodowe, które mają być egzekwowane na poziomie krajowym, muszą zostać dostosowane w „odpowiednim i proporcjonalnym ustawodawstwie krajowym". Jednak traktatom międzynarodowym nie jest łatwo ustanowić „wspólne definicje przestępstw, (i)… procedur bezpieczeństwa". Chociaż nikt nie będzie się sprzeciwiał potrzebie ustanowienia skutecznych środków zwalczania cyberprzestępczości, konieczne jest, aby wszelkie takie środki w żaden sposób nie naruszały praw obywateli do prywatności i wolności jednostki.

Prawo międzynarodowe

Ustawodawcy i organy ścigania na całym świecie opowiadają się za potrzebą przepisów prawa cybernetycznego napisanych w języku cybernetycznym. Oznacza to, że przepisy prawne wyraźnie określają cyberprzestępstwa i w pełni popierają akceptację dowodów cybernetycznych. Organy międzynarodowe, odpowiadając na to wezwanie, zwołały i opracowały traktaty i konwencje, które niestety nie dały całkowitej akceptacji państwom członkowskim. Udział kraju w określonej umowie międzynarodowej staje się skuteczny tylko wtedy, gdy zostaną opracowane i zatwierdzone przepisy krajowe, które regulują cel podpisanej umowy międzynarodowej. Oczywiście z biegiem czasu coraz więcej krajów ogłasza prawa cybernetyczne

Europa

W Europie w 2004 r. Rada Europy zaakceptowała projekt Traktatu o cyberprzestępczości, który został zaproponowany krajom na całym świecie. Podczas gdy wiele krajów zostało sygnatariuszami traktatu, tylko kilka faktycznie ogłosiło przepisy krajowe zgodne z traktatem. Interesujące jest, aby traktat w artykule 47 stanowił: „Wypowiedzenie: każda ze Stron może w dowolnym czasie wypowiedzieć niniejszą konwencję w drodze notyfikacji skierowanej do Sekretarza Generalnego Rady Europy". Artykuł 27 stanowi: „Wnioski o wzajemną pomoc na podstawie niniejszego artykułu będą wykonywane zgodnie z procedurami określonymi przez Stronę wzywającą, chyba że jest to niezgodne z prawem Strony wezwanej. Strona wezwana może… odmówić udzielenia pomocy ". Później w 2006 r. Do traktatu dołączono kontrowersyjne uzupełnienie [4], które przyciągnęło mniejszą liczbę krajów sygnatariuszy. Dodatek dotyczył strachu przed pojawieniem się ksenofobicznej troski Internet. Podsumowując, rozpoczęła się inicjatywa Rady Europy sposób na ustawodawstwo krajowe dotyczące cyberprzestępczości w wielu krajach i został wykorzystany jako motywacja do podobnego traktatu w ONZ.

Organizacja Narodów Zjednoczonych

Organizacja Narodów Zjednoczonych (ONZ) w 2010 r. Otrzymała propozycję zalecającą Traktat o cyberprzestrzeni dla członków ONZ. Po długiej debacie propozycja została odrzucona, ponieważ zawierała niedopuszczalne artykuły. Większość kontrowersji wywołały następujące artykuły:

• Artykuł 2 wniosku wskazywał na przewagę takiego traktatu nad przepisami krajowymi, stwierdzając, że „Poważne zbrodnie przeciwko pokojowi i bezpieczeństwu w cyberprzestrzeni powinny być uznawane za przestępstwa na mocy prawa międzynarodowego na mocy traktatu o cyberprzestrzeni na szczeblu Narodów Zjednoczonych, niezależnie od tego, czy były karalne czy nie. zgodnie z prawem krajowym ". Ten fragment został uznany za dwuznaczny i obraźliwy dla suwerenności narodowej.

• W art. 3.8.3, odnoszącym się do odpowiednika traktatu Unii Europejskiej, stwierdzono, że „Dane… danych o ruchu internetowym i danych transakcyjnych, zwykle telekomunikacji, wiadomości e-mail i odwiedzanych witryn [należy zachować] Celem zatrzymywania danych jest analiza danych o ruchu i masowe nadzór danych… " Wniosek sugerował, że dane należy przechowywać „przez okres od sześciu miesięcy do dwóch lat". Artykuł ten spotkał się z sprzeciwem wielu lokalnych i międzynarodowych organizacji działających na rzecz wolności obywatelskich, które uznały to sformułowanie za obraźliwe, szczególnie za „masową inwigilację danych" i wyraźne naruszenie podstawowych praw obywatelskich, których kamieniem węgielnym jest prywatność w komunikacji osobistej.

• Artykuł 4 był najbardziej kontrowersyjny. W efekcie w tym artykule wzywa się państwa członkowskie do zaakceptowania Międzynarodowego Trybunału Karnego jako super-arbitra w cyberprzestępstwach, stwierdzając:

„Każdy, kto popełni którekolwiek z przestępstw… będzie podlegał ściganiu przez sąd… Maksymalny okres pozbawienia wolnościma 30 lat i może zostać nałożony wyrok dożywocia ".

Tak więc ONZ pozostaje idealnym międzynarodowym forum do dyskusji i wymiany pomysłów, ale nie jest idealny do zawarcia międzynarodowego konsensusu. Jednak umowy dwustronne lub regionalne bardzo często wystarczają do podpisania traktatów globalnych. Europol jest przykładem.

NATO

Organizacja Traktatu Północnoatlantyckiego (NATO) , mając na uwadze przede wszystkim obronę i bezpieczeństwo, również obserwuje globalną rolę na arenie cyberbezpieczeństwa. Artykuł pojawiający się na stronie internetowej cyberbezpieczeństwa NATO. Centrum sugeruje, że „Globalne bezpieczeństwo cybernetyczne [może być] Niszą dla NATO". Zainteresowaniem NATO jest cyberterroryzm i cyberwarfare, ale drzwi do cyberprzestępczości pozostały otwarte, jak stwierdzono w polityce bezpieczeństwa cybernetycznego organizacji. Chociaż w wielu państwach członkowskich NATO Internet jest szeroko wykorzystywany, nie odgrywa żadnej roli w ich bezpieczeństwie narodowym, ani nie stanowi absolutnego filaru społecznego ani gospodarczego. Dlatego postawa członkostwa nie będzie jednolita wobec inwestowania przeciwko cyberterroryzmowi lub cyberwarfare, biorąc pod uwagę „dominującą niechęć narodów [członkowskich] do angażowania się w [kosztowne] wiążące inicjatywy międzynarodowe". W sformułowaniu w 2011 r. Strategicznej koncepcji sojuszu na rzecz obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego przyjętej przez szefów państw i rządów w Lizbonie kwestię bezpieczeństwa cybernetycznego rozwiązano w następujący sposób:

Artykuł 12. Cyberataki stają się coraz częstsze, bardziej zorganizowane i bardziej kosztowne w związku ze szkodami, jakie wyrządzają administracjom rządowym, przedsiębiorstwom, gospodarkom, a potencjalnie także sieciom transportowym i dostawom oraz innej krytycznej infrastrukturze; mogą osiągnąć próg, który zagraża dobrobytowi krajowemu i euroatlantyckiemu, bezpieczeństwu i

stabilności. Zagraniczne służby wojskowe i wywiadowcze, zorganizowani przestępcy, grupy terrorystyczne i / lub ekstremistyczne mogą być źródłem takich ataków.

Sojusz utrzymuje Centrum Doskonałości Obrony Bezpieczeństwa Cybernetycznego w Tallinie w Estonii, którego misją jest „zwiększenie zdolności, współpracy i wymiany informacji między NATO, narodami NATO i partnerami w zakresie cyberobrony… [i] być głównym źródłem wiedzy specjalistycznej w dziedzina kooperacyjnej cyberobrony… w ramach NATO, narodów i partnerów NATO ". Na ostatniej konferencji poświęconej cyberbezpieczeństwu w Centrum przedstawiono dziesięć zasad, które stanowią podstawę skutecznej cyberobrony na szczeblu suwerennego państwa. Druga zasada jest jednak całkowicie nie do przyjęcia, ponieważ obwinia sektor publiczny państwa za działanie, które mogło zostać zainicjowane przez nieuczciwą lub tajną organizację działającą w tym państwie.

1. Zasada terytorialności: infrastruktura informacyjna znajdująca się na terytorium państwa podlega suwerenności terytorialnej tego państwa.

2. Zasada odpowiedzialności: fakt, że cyberatak został przeprowadzony z systemu informatycznego znajdującego się na terytorium państwa, świadczy o tym, że czyn można przypisać temu państwu.

3. Zasada współpracy: fakt, że cyberatak został przeprowadzony za pośrednictwem systemów informatycznych znajdujących się na terytorium państwa, stwarza obowiązek współpracy z państwem ofiary.

4. Zasada samoobrony: Każdy ma prawo do samoobrony.

5. Zasada ochrony danych: Dane monitorowania infrastruktury informacyjnej są postrzegane jako dane osobowe, chyba że postanowiono inaczej (powszechna interpretacja w UE).

6. Zasada obowiązku zachowania ostrożności: każdy ma obowiązek zapewnienia rozsądnego poziomu bezpieczeństwa w swojej infrastrukturze informatycznej.

7. Zasada wczesnego ostrzegania: istnieje obowiązek powiadomienia potencjalnych ofiar o znanym, nadchodzącym cyberbezpieczeństwie.

8. Zasada dostępu do informacji: Społeczeństwo ma prawo być informowanym o zagrożeniach dla ich życia, bezpieczeństwa i dobrobytu.

9. Reguła kryminalna: Każdy naród ma obowiązek zawrzeć w swoim prawie karnym najczęstsze cyberprzestępstwa.

10. Zasada mandatu: Zdolność organizacji do działania (i regulowania) wynika z jej mandatu.

INTERPOL

Międzynarodowa Organizacja Policji Kryminalnej (INTERPOL) „jest największą międzynarodową organizacją policji na świecie, z 190 krajami członkowskimi… [z wybitną] zaawansowaną technologicznie infrastrukturą wsparcia technicznego i operacyjnego" . INTERPOL odgrywa wiodącą rolę w szkoleniu organów ścigania na całym świecie w zakresie najlepszych sposobów obrony przed cyberatakami i złośliwym oprogramowaniem, koncentrując się na

•Analiza trendów cyberataków

•Praktyczne wykorzystanie cyfrowych narzędzi kryminalistycznych w incydentach cyberbezpieczeństwa

•Techniki analizy dowodów i odzyskiwania

•Analiza techniczna złośliwego oprogramowania i botnetów

INTERPOL utrzymuje międzynarodowy sojusz cyberbezpieczeństwa na pierwszej linii obrony - organy ścigania - mające na celu

• Promowanie wymiany informacji między krajami członkowskimi poprzez regionalne grupy robocze i konferencje

• Prowadzenie szkoleń w celu budowania i utrzymywania standardów zawodowych

• Koordynacja i wspieranie operacji międzynarodowych

• Ustanowienie globalnej listy oficerów kontaktowych dostępnych przez całą dobę do celów dochodzeń w sprawie cyberprzestępczości

• Pomoc krajom członkowskim w przypadku ataków cybernetycznych lub dochodzeń w sprawie cyberprzestępczości za pośrednictwem usług śledczych i baz danych

• Rozwijanie strategicznych partnerstw z innymi organizacjami międzynarodowymi i organami sektora prywatnego

• Identyfikacja pojawiających się zagrożeń i dzielenie się tymi danymi wywiadowczymi z krajami członkowskimi

• Zapewnienie bezpiecznego portalu internetowego umożliwiającego dostęp do informacji operacyjnych i dokumenty

Utrudnienia dla egzekwowania prawa w cyberprzestrzeni

Międzynarodowe traktaty mogą zostać sporządzone i podpisane, a miejmy nadzieję, że nastąpi po nich publikacja krajowych przepisów, które skutecznie zajmą się cyberprzestępczością. To tylko część pierwsza w niekończącej się walce z cyberprzestępczością. Część druga dotyczy faktycznego usunięcia cyberprzestępców ze społeczeństwa. Obecnie istnieje kilka obszarów, które wymagają definicji lub ulepszenia, a niektóre z nich wymieniono poniżej.

• Biurokracja narodowa. W większości krajów systemy sądowe są przeciążone, a sprawy mają być rozpatrywane rok lub dwa lata po sformalizowaniu i złożeniu oskarżenia. Do tego czasu oskarżeni, jeśli są winni, mogą mieć prawo do popełniania większej liczby cyberprzestępstw.

• Sędziowie o umiejętnościach cybernetycznych. Najczęściej przestępstwa popełnione w cyberprzestrzeni obejmują włamania do sieci i naruszenia bezpieczeństwa, które są częścią wysoce wyrafinowanych programów oszustw. Sędziowie bez specjalnego i ustawicznego szkolenia mogą nie rozumieć, dlaczego oskarżony jest winny lub niewinny zarzutów.

• Uwierzytelnianie dowodów. Jeśli nagłówek wiadomości e-mail zawiera adres e-mail oskarżonego, to samo w sobie niekoniecznie jest dowodem winy lub niewinności.

• Utrata dowodów. Przy dużej luce między popełnieniem domniemanego przestępstwa a sądowym rozpoznaniem sprawy dowody elektroniczne mogą zostać utracone lub zmienione.

• Dostęp do dowodów. Dowody mogą znajdować się na serwerach w obcym kraju i mogą być wymagane specjalne procedury ekstradycji danych.

• Kompleksowe prawodawstwo. Ponieważ programy cyberprzestępczości wyprzedzają organy ścigania o kilka miesięcy, do procesu wprowadzane są dodatkowe opóźnienia.

• śledczy w sprawie cyberprzestępczości. Wraz z eksplozją Internetu i równoległą eksplozją cyberprzestępczości nie ma na świecie kraju, który miałby wystarczającą liczbę pracowników policji cybernetycznej do prowadzenia każdego przypadku domniemanej cyberprzestępczości.

Według wszystkich standardów cyber legalny system jest w stanie embrionalnym. Jednak poprawia się na całym świecie i jest to uzasadnione mam nadzieję, że cyberprzestępczość zostanie powstrzymana w najbliższej przyszłości.

Przepisy dotyczące cyberprzestrzeni w Stanach Zjednoczonych

Przed stworzeniem cyberprzestrzeni, jaką znamy dzisiaj, istniała inna przestrzeń kosmiczna - choć nie została zidentyfikowana jako taka - Dataspace. Dzięki postępom w fizyce i chemii półprzewodników komputery analogowe przekształciły się w cyfrowe, a rozmiar sprzętu zaczął się zmniejszać, stopniowo osiągając dzisiejszy rozmiar i moc obliczeniową. Dataspace - era cyfrowego przechowywania informacji - rozpoczęła się w latach sześćdziesiątych i w połowie lat siedemdziesiątych. Wiele firm zaczęło mieć minikomputery do ich obsługi i rachunkowości , a jednocześnie zaczęły pojawiać się obawy dotyczące prywatności danych i bezpieczeństwo komputerowe, co skutkuje ogłoszeniem przepisów dotyczących ochrony danych, prywatności i bezpieczeństwa narodowego.

Krajowa ustawa o ochronie cybernetycznej z 2014 r

Krajowa ustawa o cyberbezpieczeństwie i ochronie infrastruktury krytycznej z 2014 r. Jest fundamentalnym prawem Stanów Zjednoczonych, które w pełni zajmuje się Internetem i możliwymi zagrożeniami, z którymi się wiąże, mające na celu „Zabezpieczenie Nation Against Cyber Attack. ” Najważniejsze jest to, że prawo zawiera definicję prawną tego, czym jest „incydent cybernetyczny”. Mianowicie „incydent cybernetyczny” jako incydent lub próba spowodowania incydentu, który, jeśli się powiedzie,: (1) zagrozi bezpieczeństwu, integralności, poufności, lub dostępność systemu informacyjnego lub sieci lub jakichkolwiek informacji przechowywane w takim systemie, przetwarzane w nim lub przejeżdżające przez niego; (2) naruszają prawa lub procedury związane z bezpieczeństwem systemu, polityką dopuszczalnego użytkowania lub aktami terroryzmu wymierzonymi przeciwko takiemu systemowi lub sieci; lub (3) odmawiać dostępu do lub degradować, zakłócać lub niszczyć taki system lub sieć, lub porażki w działaniu lub kontroli technicznej takiego systemu lub sieci. Prawo wprowadza National Institute of Standards and Technology (NIST) w celu ułatwienia publiczno-prywatnej współpracy w zakresie bezpieczeństwa cybernetycznego w celu opracowania dobrowolnego, kierowanego przez przemysł zestawu standardów i procesów w celu zmniejszenia ryzyka cybernetycznego infrastruktury krytycznej. Ustawa zmienia również Ustawę o bezpieczeństwie wewnętrznym, dodając przepisy zatytułowane Ustawa o bezpieczeństwie wewnętrznym w zakresie cyberbezpieczeństwa, które rozwijają kategorie zawodowe w zakresie bezpieczeństwa cybernetycznego - po raz pierwszy w rządzie federalnym. W skrócie, prawo uznaje potrzebę stworzenia armii cyberbezpieczeństwa.

Ustawa o ocenie siły roboczej z cyberbezpieczeństwa z 2014 r

Ustawa o ocenie siły roboczej w cyberbezpieczeństwie - kieruje sekretarz Sekretarz Bezpieczeństwa Wewnętrznego, aby przeprowadzić ocenę cyberbezpieczeństwa, personel Departamentu Bezpieczeństwa Wewnętrznego (DHS), który powinien zawierać informacje na temat

• Gotowość i zdolność takiej siły roboczej do wypełnienia misji bezpieczeństwa cybernetycznego;

• Gdzie stanowiska pracowników cyberbezpieczeństwa znajdują się w DHS;

• Które takie stanowiska są wykonywane przez stałych pełnoetatowych pracowników DHS, niezależnych wykonawców oraz osoby zatrudnione przez inne agencje federalne;

• Które z tych stanowisk są wolne

• Odsetek osób w każdej kategorii bezpieczeństwa cybernetycznego i specjalizacji, które zostały przeszkolone w zakresie wykonywania pracy; i

• W jakich przypadkach takie szkolenie nie zostało przeprowadzone, jakie wyzwania napotkano na temat zapewnienia takiego szkolenia.

Ustawa o rekrutacji i zatrzymaniu pracowników w zakresie cyberbezpieczeństwa z 2014 r

Jest to bardzo ważne prawo, ponieważ upoważnia Sekretarza Departamentu Bezpieczeństwa Wewnętrznego w celu ustalenia stanowisk w Departamencie Bezpieczeństwa Wewnętrznego (DHS) niezbędnych do wykonywania obowiązków związanych z cyberbezpieczeństwem. Ponadto wymaga od DHS dostarczenia rządowi wskazówek identyfikujących ostre i pojawiające się niedobory umiejętności w zakresie cyberbezpieczeństwa.

Ustawa o ochronie prywatności w prawie handlowym z 2011 r

Celem tego aktu jest „Ustanowienie ram regulacyjnych dla kompleksowej ochrony danych osobowych osób fizycznych pod egidą Federalnej Komisji Handlu i do innych celów". Zostało to uznane za

• Rozpowszechnianie informacji umożliwiających identyfikację osób (PII) budzi obawy, że może to prowadzić do kompromisów w zakresie prywatności danych, bezpieczeństwa danych i równie ważnej integralności danych.

• Nadużycie w gromadzeniu, przechowywaniu, dystrybucji i wykorzystywaniu danych osobowych spowodowało już wiele różnych przestępstw, głównie cyberprzestępstw, co negatywnie wpłynęło na rozwój wiarygodnego handlu elektronicznego.

• Brakuje, a jednocześnie potrzeba ram prawnych zapewni to jednolite i kompleksowe stanowisko rządu w odniesieniu do postępowania z danymi osobowymi.

Biorąc pod uwagę powyższe, amerykańscy prawodawcy opracowali i uchwalił to prawo, które kieruje prokuratorami generalnymi pięćdziesięciu stanów wraz z Federalną Komisją Handlu (FTC) w celu ustalenia szczegółowych zasady jednolitego systemu prawnego obejmującego cały stan, który będzie chronił informacje osobowe w ramach kompleksowy sposób. Najważniejsze cechy tego prawa są następujące:

• Odpowiedzialność. Wszystkie podmioty objęte tym podmiotem ochrony danych osobowych w trakcie prowadzenia działalności gospodarczej - muszą „ponosić odpowiedzialność zarządczą [za dane znajdujące się pod ich opieką]". W obecnym kontekście odpowiedzialność kierownictwa za dane oznacza istnienie zasad dotyczących gromadzenia, przetwarzania, przechowywania, bezpieczeństwa fizycznego i wirtualnego, dystrybucji na rzecz osób trzecich oraz wykorzystywania danych zaklasyfikowanych jako informacje umożliwiające identyfikację osób.

• Prywatność od samego początku. We wszystkich aspektach przetwarzania danych priorytetem musi być prywatność danych. Można to osiągnąć, stosując „odpowiednie procesy i praktyki zarządzania w całym cyklu życia danych".

• Przejrzystość. Osoby gromadzące dane, zarówno w cyberprzestrzeni, jak i gdzie indziej, muszą „zapewniać jasne, zwięzłe i terminowe zawiadomienie osób fizycznych" w zakresie zarządzania zebranymi danymi PII.

• Indywidualny udział. Posiadacze danych osobowych muszą „oferować osobom fizycznym solidny, przejrzysty i rzucający się w oczy mechanizm", aby umożliwić lub zabronić korzystania z ich informacji osobowych i móc w dowolnym momencie zmienić ten status.

• Minimalizacja danych. Dane dotyczące osoby fizycznej, gromadzone w trakcie świadczenia usługi, muszą zostać zminimalizowane i muszą być „takie, jak jest to uzasadnione".

• Ograniczenia w dystrybucji informacji. Osoby zbierające dane osobowe przekazujące takie dane stronom trzecim muszą „wymagać na mocy umowy, aby taka strona trzecia" w pełni przestrzegała tego prawa w zakresie zarządzania danymi. Ponadto przekazywanie danych osobowych do „niewiarygodnych stron trzecich [jest] zabronione".

• Integralność danych. Osoby zbierające dane osobowe muszą dołożyć wszelkich starań, poprzez odpowiednie zasady, praktyki i mechanizmy, aby zapewnić, że wykorzystywane „dane osobowe […] są dokładne [zwłaszcza, gdy takie informacje]… mogą być wykorzystane do odmowy konsumentom korzyści lub wyrządzenia znacznej szkody".

• Egzekwowanie i kary. Ustawa ta nakazuje FTC ogłaszanie przepisów dotyczących wiedzy i dążenie do ich egzekwowania. Kary będą oparte na skali naruszeń i czasie, przez jaki naruszenia te zostały popełnione.

• Przepisy dotyczące bezpiecznej przystani. Prawo przyznaje FTC uprawnienia do wprowadzania programów „bezpiecznej przystani". Bezpieczna przystań to termin prawny odnoszący się do zmiany, zmniejszenia lub zniesienia zobowiązań strony w stosunku do przepisów określonych przepisów prawa. Takie odstępstwa od zobowiązań prawnych rozciągają się na nazwę większego dobra. Programy takie miałyby zastosowanie do podmiotów zbierających dane, podlegających jurysdykcji tego prawa, dopóki intencja tego prawa pozostaje w mocy, czyli ochrona prywatności jednostki.

Ustawa o ochronie prywatności w prawie handlowym z 2011 r.

Nie przewiduje szczegółowych zasad dotyczących kwestii zarządzania danymi osobowymi, ale upoważniają one FTC, która nadzoruje handel i najlepiej nadaje się do takiego zadania, do opracowywania zasad i środków, które ostatecznie ochronią dane osobowe i zminimalizują nadużycia i cyberprzestępczość.

Ustawa o cyberbezpieczeństwie z 2010 r

Celem tego aktu jest zapewnienie ciągłego swobodnego przepływu handlu w Stanach Zjednoczonych i ze swoimi globalnymi partnerami handlowymi poprzez bezpieczną komunikację cybernetyczną, zapewnienie dalszego rozwoju i wykorzystania Internetu i komunikacji intranetowej do takich celów, aby zapewnić rozwój kadry specjalistów w dziedzinie technologii informatycznych w celu poprawy i utrzymania skutecznej obrony cyberbezpieczeństwa przed zakłóceniami oraz do innych celów.

Zostało to uznane za

• Cyberprzestrzeń jest integralną częścią społeczeństwa amerykańskiego i bardzo ważną infrastrukturą dla wszystkich aspektów życia, przy czym Biały Dom określa ją jako strategiczny atut narodowy.

• Internet nie jest tak bezpieczny, jak powinien, biorąc pod uwagę z jednej strony jego znaczenie i wartość dla Stanów Zjednoczonych, az drugiej rosnące zagrożenia w postaci cyberprzestępczości i ataków terrorystycznych.

• Potrzebna jest kompleksowa strategia bezpieczeństwa narodowego, a także poprawa jakości i ilości cyberbezpieczeństwa

Zainteresowani powyższymi obawami amerykańscy prawodawcy opracowali i uchwalili to prawo, kierując jego wdrażanie raczej do prezydenta USA niż do agencji rządowej, jak w większości przypadków.

Oto główne punkty prawa:

• Certyfikaty. Prawo dotyczy zapotrzebowania na wykwalifikowanych specjalistów ds. Bezpieczeństwa cybernetycznego, czego warunkiem wstępnym jest „akredytacja, szkolenie i programy certyfikacji w zakresie bezpieczeństwa cybernetycznego".

• Stypendia cyberbezpieczeństwa. Prawo nakazuje Narodowej Fundacji Nauki, by „ustanowiła Federalny program stypendiów cybernetycznych służący rekrutacji i szkoleniu nowej generacji specjalistów w dziedzinie technologii informatycznych". Program ma zapewnić 1000 absolwentów i studentów pełnych stypendiów rocznie na programy prowadzące do cyberbezpieczeństwa. Co więcej, talentów należy szukać nawet wśród uczniów szkół średnich, „w celu promowania świadomości bezpieczeństwa komputerowego w klasach średnich i licealnych".

• Konkursy cyberbezpieczeństwa. Prawo nakazuje Narodowemu Instytutowi Standardów i Technologii ustanawiać konkursy z zakresu bezpieczeństwa cybernetycznego i inne wyzwania z nagrodami, aby „przyciągać, identyfikować, oceniać i rekrutować utalentowane osoby do federalnej siły roboczej w dziedzinie technologii informatycznych… [oraz w celu]… stymulować innowacje w podstawowych i stosowanych badaniach w zakresie bezpieczeństwa cybernetycznego. "

• Plan siły roboczej w zakresie bezpieczeństwa cybernetycznego. Uznając, że cyberbezpieczeństwo wymaga cyber-wojowników, prawo uwzględnia potrzebę opracowania planu dla każdej agencji rządowej, który zapewni jakość i ilość w jej cyberobronie. Plan obejmuje „prognozy dotyczące zatrudniania w dziedzinie cyberbezpieczeństwa… długoterminowe i krótkoterminowe planowanie strategiczne mające na celu zaradzenie niedoborom umiejętności krytycznych… strategie rekrutacji… szkolenia związane z cyberbezpieczeństwem", tak aby cyberprzestrzeń była bezpieczna.

• Wskazówki dotyczące bezpieczeństwa cybernetycznego NIST. Prawo uznaje National Institute of Standards and Technology (NIST) za autorytet technologiczny w obszarze cyberprzestrzeni i cyberbezpieczeństwa i zaleca mu „promowanie kontrolowanych, opracowanych przez sektor prywatny technik pomiaru ryzyka cyberbezpieczeństwa, środków zarządzania ryzykiem i najlepszych praktyk", które mogą później służą jako standardy oceny gotowości do cyberbezpieczeństwa.

• Rozwój wiedzy w zakresie cyberbezpieczeństwa. Prawo podkreśla potrzebę ciągłego rozwoju wiedzy, umiejętności i specjalistów posiadających wiedzę specjalistyczną w zakresie projektowania „złożonych systemów wymagających dużego oprogramowania, które są bezpieczne i niezawodne… [które] gwarantują prywatność tożsamości, informacji lub legalnych transakcji. "

• Panel doradczy ds. Cyberbezpieczeństwa. Ustawiając prezydenta jako centralny punkt jego realizacji, prawo wzywa do utworzenia panelu złożonego z wykwalifikowanych „przedstawicieli przemysłu, organizacji akademickich, organizacji non-profit, grup interesu i organizacji rzeczniczych", które będą

doradzać prezydentowi w „sprawach odnoszące się do krajowego programu i strategii bezpieczeństwa cybernetycznego. ”

Ustawa o cyberbezpieczeństwie z 2010 r.

Stanowi punkt wyjścia dla stworzenia planu podnoszenia świadomości w zakresie bezpieczeństwa cybernetycznego, który dzięki polityce, wytycznym i dużym środkom zapewni wykwalifikowanych specjalistów ds. bezpieczeństwa cybernetycznego, którzy będą bronić zarówno sektora publicznego, jak i prywatnego przed cyberprzestępczością i cyberbezpieczeństwem.

Federalna ustawa o zarządzaniu bezpieczeństwem informacji z 2002 r

W 1987 r. Amerykańscy prawodawcy, widząc wzrost przetwarzania danych i rosnące wykorzystanie komputerów, uchwalili ustawę - Computer Security Act z 1987 r. - która zapewniła pewne podstawowe, według dzisiejszych standardów, wytyczne dotyczące bezpieczeństwa i ogólnego traktowania danych. W 2002 roku uświadomiono sobie, że zagrożenia zostały pomnożone przez kilka rzędów wielkości oraz zarządzanie bezpieczeństwem systemów i danych wymagało zorganizowanego podejścia. Federalna ustawa o zarządzaniu bezpieczeństwem informacji (FISMA) ustanawia standardy, które muszą spełnić agencje federalne i federalni kontrahenci, które są wymierne i mierzalne. FISMA poleca szefom agencji ustanowienie i wdrożenie polityk i procedur w celu zminimalizowania ryzyka i zagrożeń dla rządowych systemów informacyjnych. Odpowiedzialność za stworzenie niezbędnych standardów spoczywała na NIST, w celu zapewnienia jednolitych standardów bezpieczeństwa informacji w całym rządzie, które zapewnią integralność, dostępność i bezpieczeństwo danych. FISMA stanowi kamień milowy w formułowaniu zasad zgodności w zakresie bezpieczeństwa informacji, a jego cel obejmuje następujące cele:

• Zapewnienie kompleksowych ram dla zapewnienia skuteczności kontroli bezpieczeństwa informacji nad zasobami informacji, które wspierają operacje federalne i zasoby

• Zapewnienie rozwoju i utrzymania minimalnych kontroli wymaganych do ochrony federalnych informacji i systemów informatycznych

• Zapewnienie mechanizmu lepszego nadzoru nad programami bezpieczeństwa informacji agencji federalnych

• Uznanie, że wybór konkretnych technicznych rozwiązań w zakresie bezpieczeństwa informacji o sprzęcie i oprogramowaniu należy pozostawić indywidualnym agencjom spośród produktów opracowanych na rynku

Najważniejsze cechy FISMA są następujące:

• Obowiązki. Prawo nakłada na szefa agencji wszelkie obowiązki związane z zapewnieniem bezpieczeństwa wszystkich informacji znajdujących się pod nadzorem agencji, gdzie poziom bezpieczeństwa powinien być „współmierny do ryzyka i wielkości szkody wynikającej z nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacja lub zniszczenie ”przechowywanych informacji.

• Planowanie. Agencje mogą opracować własny program bezpieczeństwa w celu ochrony swoich informacji, nawet jeśli ich informacje nie znajdują się w ich własnych lokalach - dotyczy to wykonawców i stron satelitarnych.

• Raportowanie. Zgodność z duchem i listem FISMA zostanie wykazana w rocznym raporcie, który szef każdej agencji przygotuje, wraz z dystrybucją obejmującą:

• Dyrektor FISMA w Departamencie Handlu

• Domowe komisje ds. Reformy rządu i nauki

• Senackie komisje spraw rządowych, handlu, nauki i transportu

• Komisje ds. Środków

• Biuro Generalnego Kontrolera (OCG). OCG poświadczy „na temat adekwatności i skuteczności polityk, procedur i praktyk bezpieczeństwa informacji oraz zgodności z wymogami… [FISMA]".

• Niezależne oceny. Każdego roku każda agencja będzie podlegać niezależnej ocenie przeprowadzonej przez Generalnego Inspektora Agencji „powołanego na podstawie Ustawy Generalnej Inspektora z 1978 r.… Lub przez niezależnego audytora zewnętrznego, zgodnie z ustaleniami Generalnego Inspektora agencji".

Raport FISMA z 2010 r. Komisji Papierów Wartościowych i Giełd (SEC), agencji rządu federalnego, można obejrzeć online]. Raport przygotowany przez niezależnego kontrahenta zawiera ustalenia Generalnego Inspektora ze szczegółowymi zaleceniami dotyczącymi ulepszenia systemu informacyjnego SEC pod względem bezpieczeństwa danych.

US PATRIOT Act z 2001 roku

Cel USA PATRIOT (Zjednoczenie i wzmocnienie Ameryki poprzez zapewnienie odpowiednich narzędzi wymaganych do przechwytywania i

Ustawą o przeciwdziałaniu terroryzmowi, znaną również jako Ustawa o patriocie, jest „Odstraszyć

i karać akty terrorystyczne w Stanach Zjednoczonych i na całym świecie,

ulepszyć narzędzia dochodzeniowe organów ścigania i do innych celów. " Ustawa ta została zaproponowana i uchwalona w następstwie ataków z 11 września na własność publiczną i prywatną w Stanach Zjednoczonych. Jest to bardzo kontrowersyjna ustawa, która ogranicza dotychczasowe swobody obywatelskie w imię bezpieczeństwa narodowego. Poniżej znajdują się kwestie, które to prawo odnosi się do gromadzenia i przetwarzania informacji.

• Krajowa grupa zadaniowa ds. Przestępstw elektronicznych. Uznając potrzebę informacji w walce z przestępczością, a w szczególności z terroryzmem, prawo kieruje tworzeniem „krajowej sieci elektronicznych grup zadaniowych ds. Przestępczości… w celu zapobiegania, wykrywania i badania różnych form elektronicznych przestępstwa, w tym potencjalne ataki terrorystyczne na infrastrukturę krytyczną i systemy płatności finansowych ".

• Przechwytywanie informacji. Prawo przyznaje uprawnienia do rozpoznania amerykańskich agencji rządowych „do przechwytywania przekazów elektronicznych, ustnych i elektronicznych związanych z terroryzmem, oszustwami komputerowymi i przestępstwami polegającymi na nadużyciach". Może wystąpić „przejęcie wiadomości poczty głosowej na podstawie nakazów".

• Ujawnianie zapisów. Dostawca usług internetowych „może ujawnić zapis lub inne informacje dotyczące subskrybenta lub klienta… jeżeli dostawca ma uzasadnione przekonanie, że nagły wypadek, który wiąże się z bezpośrednim zagrożeniem śmierci lub poważnych obrażeń fizycznych, wymaga natychmiastowego ujawnienia informacji".

• Oszustwa telemarketingowe. Prawo dotyczy charytatywnych oszustw telemarketingowych i wymaga pełnego ujawnienia takich działań

„Nazwa i adres pocztowy organizacji charytatywnej, w imieniu której dokonywane jest nagabywanie”.

Ustawa Patriot koncentruje się głównie na środkach pomagających federalnym organom ścigania w walce z terroryzmem i finansowymi przestępstwami. Chociaż grupy wolności obywatelskich twierdziły, że wiele przepisów ustawy jest niezgodnych z konstytucją i że ustawa „rozszerzyła władzę rządu na wtrącanie się w życie prywatne ludzi z niewielkimi lub żadnymi dowodami wykroczeń”, ustawę przedłużono do 1 czerwca 2015 r.

Communications Assistance for Law Enforcement Act z 1994 r.

Ustawa o pomocy prawnej w zakresie egzekwowania prawa z 1994 r (w skrócie CALEA) wymaga, aby firmy z sektora telekomunikacyjnego zapewniały organom ścigania dostęp do prywatnej komunikacji i zapisów takiej komunikacji. Ustawa należy do Federalnej Komisji Łączności (FCC). „W odpowiedzi na obawy, że pojawiające się technologie, takie jak komunikacja cyfrowa i bezprzewodowa, utrudniają organom ścigania wykonywanie autoryzowanego nadzoru, Kongres uchwalił CALEA 25 października, 1994. ” Jednak branża telekomunikacyjna nie zaprojektowała ani nie zbudowała swoich obiektów i usług w sposób konieczny, aby sprostać temu celowi, i potrzebna jest dodatkowa infrastruktura, aby „spełnić określone przez prawo obowiązki CALEA”. Poniżej znajdują się główne punkty aktu

• Wymagania. Firmy telekomunikacyjne świadczące usługi

publiczność musi być w stanie przechwycić „wszelką komunikację przewodową i elektroniczną prowadzoną przez przewoźnika… subskrybenta…”. Stwierdzono, że ta usługa dla organów ścigania musi być „… na podstawie orzeczenia sądowego lub innego zgodnego z prawem upoważnienia…”

• Koszt zgodności. Najwyraźniej instalacja sprzętu, który ułatwi wdrożenie CALEA, wiąże się z wysokimi kosztami, których firmy telekomunikacyjne nie są w stanie ponieść.

• Szyfrowanie. Jeżeli abonent zastosuje własną technologię szyfrowania, „Operator telekomunikacyjny nie ponosi odpowiedzialności

do odszyfrowywania,… chyba że szyfrowanie zostało dostarczone przez przewoźnika, a przewoźnik posiada informacje niezbędne do odszyfrowania komunikacji. ”

• Pojemność. Inną kwestią jest zdolność przechwytywania, którą firma telekomunikacyjna powinna utrzymywać, która „będzie oparta na rodzaju sprzętu, rodzaju usługi, liczbie abonentów, rodzaju lub wielkości lub operatora, charakterze obszaru usług lub jakimkolwiek innym środku; i określa, w maksymalnym możliwym zakresie, pojemność wymaganą w określonych lokalizacjach geograficznych. ”

• Nieuczciwe podsłuchiwanie. Aby chronić rządową bezpieczną komunikację radiową, ustawa zabrania hakerom słuchania komunikacji, która jest „… szyfrowana lub przesyłana przy użyciu technik modulacji, których podstawowe parametry zostały

ukryte przed opinią publiczną w celu zachowania prywatności takiej komunikacji… ”

• Bezpieczny port. Zgodność z dyrektywami CALEA można odstąpić w szczególnych okolicznościach, z upoważnienia Prokuratora Generalnego USA i FCC. Zwykle takie zwolnienia przedłużają jedynie datę zgodności, aby umożliwić firmie telekomunikacyjnej odpowiednie wyposażenie.

• koszty. W telekomunikacji technologie zawsze się rozwijają, w związku z tym zgodność z CALEA spowoduje dodatkowe koszty dla odpowiednich firm, które nie są wspierane przez przychody. „Prokurator generalny może, z zastrzeżeniem dostępności środków, zgodzić się zapłacić operatorom telekomunikacyjnym wszelkie uzasadnione koszty bezpośrednio związane z modyfikacjami

dokonanymi przez przewoźników… (w celu) w celu dostosowania się do [CALEA]. Zatwierdzone środki na lata budżetowe 1995–1998 wyniosły 0,5 mld USD.

• Kary. Wspieranie organów ścigania w ich misji nie jest zadaniem dobrowolnym, ale obowiązkiem prawnym. Ustawa stanowi, że „operator telekomunikacyjny, producent urządzeń do transmisji lub przełączania telekomunikacji lub dostawca usług wsparcia telekomunikacyjnego [uznany za niezgodny z CALEA może zostać ukarany grzywną]… do 10 000 USD za każdy dzień z naruszeniem. ” Grupy wolności obywatelskich czuwające nad CALEA są bardzo zaniepokojone możliwym rozszerzeniem CALEA na telefonię internetową. „Ta ekspansja budzi poważne obawy w zakresie swobód obywatelskich, ponieważ wymagałaby od dostawców VoIP zbudowania wszystkich swoich produktów z backdoorami nadzoru, do których dostęp mają organy ścigania i prawdopodobnie będą niewłaściwie wykorzystywane przez hakerów i przestępców”.

Ustawa o bezpieczeństwie komputerowym z 1987 r.

Prawo to było prekursorem FISMA , a jego celem było poprawić „bezpieczeństwo i prywatność poufnych informacji w federalnych systemach komputerowych… [i stworzyć] sposób na ustanowienie minimalnych akceptowalnych praktyk bezpieczeństwa dla takich systemów…” Niektóre z najważniejszych przepisów prawa były następujące.

• Autorytet. Prawo wskazuje na potrzebę opracowania „standardów bezpieczeństwa komputerowego i minimalnych akceptowalnych praktyk” i przypisuje NIST do zadania z pomocą Narodowej Agencji Bezpieczeństwa.

• Program. Program ustanawia zasady, „standardy, wytyczne oraz powiązane metody i techniki dotyczące systemów komputerowych… [a także] standardy techniczne, administracyjne, fizyczne i administracyjne oraz wytyczne dotyczące opłacalnego bezpieczeństwa i prywatności wrażliwych informacji na komputerze federalnym systemy. ”

• Wcześniejsze powiązane prawo. Ustawa ta zmieniła również federalną ustawę o własności i usługach administracyjnych z 1949 r., Usprawniając ją o praktyki technologiczne i zarządcze z 1987 r.

• Trening. Prawo kładło duży nacisk na szkolenie, stwierdzając, że każda agencja federalna zapewni obowiązkowe okresowe szkolenie w zakresie świadomości bezpieczeństwa komputerowego i przyjętych praktyk bezpieczeństwa komputerowego wszystkich pracowników zaangażowanych w zarządzanie, użytkowanie lub obsługę każdego komputera federalnego system… Takie szkolenie musi być zaprojektowane

1. Zwiększenie świadomości pracowników na temat zagrożeń i podatności systemów komputerowych

2. Zachęcanie do stosowania ulepszonych praktyk bezpieczeństwa komputera

Ustawa o prywatności z 1974 r.

Na początku lat siedemdziesiątych XX wieku zdano sobie sprawę, że powiązane i przekrojone bazy danych mogą bardzo szybko zaowocować szeroką gamą zapisów dotyczących danej osoby i że należy zapobiegać nadużywaniu takiej władzy. Było to zwycięstwo grup wolności obywatelskich, które były bardzo zaniepokojone tym, że technologia bardziej pracuje nad odzyskiwaniem danych, a mniej na ochroną danych. Niektóre z najważniejszych wydarzeń aktu podążać.

• Warunki ujawnienia. Kluczową kwestią jest ujawnienie danych osobowych, a prawo stanowi, że „Żadna agencja nie ujawni żadnych zapisów zawartych w systemie zapisów za pomocą jakichkolwiek środków komunikacji z jakąkolwiek osobą lub inną agencją, z wyjątkiem pisemnego wniosku złożonego

przez, lub za uprzednią pisemną zgodą osoby, której dotyczy dokument… ” Jednak ujawnienie zapisów byłoby dozwolone do oficjalnego użytku. Klauzula ta miała na celu zablokowanie nieoficjalnego ujawnienia danych osobowych.

• Poprawka do wolności słowa. Istnieje bardzo dziwna przyczyna w prawie (zgodnie z wymogami Agencji 7), stwierdzająca, że „Każda agencja, która prowadzi system rejestrów,… nie prowadzi rejestrów opisujących, w jaki sposób poszczególne osoby wykonują prawa zagwarantowane w Pierwszej Poprawce, chyba że wyraźnie zezwalają na to ustawa lub przez osobę, o której prowadzona jest ewidencja, lub o ile nie dotyczy i jest w zakresie dozwolonego działania organów ścigania. ” Luźno wyrażone oznacza, że rząd USA nie powinien oznaczać obywateli na podstawie ich otwartości.

• Dokładność zapisów. Biorąc pod uwagę, że dokładność jest najważniejszym atrybutem zapisów, prawo wyraźnie nakazuje, aby agencje „zachowywały wszystkie zapisy… z taką dokładnością, stosownością, terminowością i kompletnością, jaka jest racjonalnie niezbędna dla zapewnienia uczciwości w ustalaniu”.

• Listy mailingowe. Na początku lat siedemdziesiątych automatyzacja danych ułatwiła tworzenie skategoryzowanych list mailingowych do celów komercyjnych, a prawo chciało upewnić się, że nie dochodzi do nadużywania danych osobowych pod nadzorem rządu. Prawo stanowi: „Nazwisko i adres osoby fizycznej nie mogą być sprzedawane ani wynajmowane przez agencję, chyba że takie działanie jest wyraźnie dozwolone przez prawo. Przepisu tego nie należy interpretować jako wymagającego nieujawniania nazwisk i adresów, które w innym przypadku mogą zostać upublicznione. ”

• Minimum zapisów. Prawo dotyczące kompilacji prywatnych niepowiązanych danych na temat osób fizycznych wyraźnie stanowi: „Każda agencja, która prowadzi system rejestrów,… zachowuje w swoich rejestrach tylko takie informacje o osobie, które są istotne i niezbędne do osiągnięcia celu agencji”.

Cyberprzestępczość

Cyberprzestępczość jest produktem ubocznym cyberprzestrzeni, służąc jako czarne piętno w optymizmie, jaki Internet dał światu. Cyberprzestępczość rośnie w ciągu ostatnich dwóch dekad, osiągając roczny poziom ponad pół miliarda dolarów w 2009 roku. „W rzeczy samej, napędzane perspektywą znacznych zysków, innowacje i techniki cyberprzestępczości wyprzedziły tradycyjne modele bezpieczeństwa i wiele obecnych technologii wykrywania opartych na sygnaturach”. Rozwinął się nowy przemysł podziemny - centra cyberprzestępczości. Są to legalne firmy zatrudniające nawet pięćdziesięciu pracowników, którzy oferują usługi internetowe, od projektowania stron internetowych i reklam internetowych po hosting stron internetowych i rejestrację nazw domen. Stopniowo te firmy zajmujące się cyberprzestępczością zmieniają setki tysięcy Internetowych hostów - komputery podłączone do Internetu – w swoje zombie przez instalowanie złośliwego oprogramowania . Instalacja złośliwego oprogramowania odbywa się pod fałszywymi pozorami. Na przykład mają szereg witryn internetowych, na których odwiedzającym oferuje się prawdopodobnie potrzebne oprogramowanie za darmo. W rzeczywistości to oprogramowanie jest złośliwym oprogramowaniem, które przekierowuje wskaźnik DNS znajdujący się w hoście na nieuczciwy, który źle kieruje interakcjami użytkownika w sieci, co skutkuje naruszeniem poufnych danych użytkownika. Zaskakujące jest to, że znaczna część cyberprzestępczości wciąż nie służy korzyściom finansowym, a jedynie szkodom. Równie zaskakujące jest to, że wiele organizacji wykorzystuje więcej zasobów do wykorzystywania Internetu przez pracowników niż do ochrony cybernetycznej. W stosunku do wymaganych zasobów cyberprzestępczość jest najbardziej opłacalnym i fizycznie bezpiecznym ze wszystkich przestępstw, a nowe zagrożenia są stale rozpoznawane. Nie jest możliwe sporządzenie kompleksowej listy przestępstw, które można popełnić przez Internet. Jeden fakt jest oczywisty, że hakerzy są zastępowani

przez przestępczość zorganizowaną i że zwiększone wydatki na obronę cybernetyczną niekoniecznie prowadzą do zwiększenia bezpieczeństwa cybernetycznego, ale priorytetem jest ryzyko.

Trendy w cyberprzestępczości

Trendy wskazują, że cyberprzestępczość nie jest jedynym cyberatakiem, a nowe bardzo innowacyjne nielegalne programy pojawiają się codziennie w Internecie. Istnieje wiele aplikacji na telefony komórkowe, które zostały zaprojektowane z myślą o bezpieczeństwie, oraz liczne aplikacje z myślą o cyberprzestępczości. Ogół społeczeństwa w dobrej wierze pobiera i instaluje aplikacje, nie wiedząc, czy są bezpieczne. W rezultacie szkodliwe aplikacje infekują zarówno pierwszy telefon, jak i te, z którymi się komunikują, a także uniemożliwiają dostęp do zawartości telefonu. Tabela 9.3 zawiera listę nadużyć cybernetycznych, które wzrosły.

Zwalczanie cyberprzestępczości

Połączenie z siecią samo w sobie stanowi lukę. Dlatego dobrą praktyką jest łączenie się z Internetem i rozłączanie się z nim w zależności od potrzeb. Łatwość popełnienia cyberprzestępczości sprawiła, że Internet, to cudowne dzieło ludzkie, stał się polem minowym. Jednak świadomość i korzystanie z oprogramowania ochronnego, takiego jak te wspomniane w rozdziale o wtargnięciach, może zminimalizować ryzyko. Filozofią walki z cyberprzestępczością powinno być nie tyle maksymalizowanie bezpieczeństwa, co minimalizowanie ryzyka. Istnieje subtelna, ale ważna różnica w tych dwóch koncepcjach, gdzie pierwsza jest tylko środkiem, a druga jest prawdziwym celem. Na poziomie korporacyjnym cyberbezpieczeństwo nie powinno być postrzegane jako ćwiczenie techniczne, ale jako najwyższe obowiązki kierownicze, które są delegowane na szefa bezpieczeństwa organizacji. W związku z tym cyberbezpieczeństwo powinno być najważniejszym projektem najwyższego kierownictwa. Istnieje wiele programów chroniących przed cyberprzestępczością, które odfiltrowują podejrzane strony internetowe i filtrują tylko wybrane strony internetowe i korespondentów e-mail. Takie oprogramowanie zapewnia „bezpieczeństwo wiadomości przychodzących i wychodzących, (wysoce) skuteczną ochronę antyspamową i antywirusową, zaawansowane filtrowanie treści, zapobieganie utracie danych i szyfrowanie wiadomości e-mail" [34]. Z cyberbezpieczeństwa żadna korporacyjna aktywność cybernetyczna nie może być uznana za nieistotną. Jednak niektóre obszary wymagają szczególnej uwagi ze względu na zwiększoną cyberprzestępczość. Jednym z takich obszarów jest zarządzanie hasłami. Znaczna część ma miejsce przy naruszonych hasłach. Przynajmniej ten rodzaj cyberprzestępczości można zwalczać, wdrażając hasła jednorazowe (OTP) [35]. Tabela 9.4 wymienia cztery obszary - słabe linki - które są na czele cyberprzestępczości. W naszych środkach obrony przed cyberprzestępczością istnieją dwa fronty. Pierwszy to nasza fortyfikacja techniczna. Oznacza to, że instalacja na naszych komputerach najlepszych możliwych programów antywirusowych. Istnieje wiele tak renomowanych programów, nawet dla smartfonów [36], telefonów komórkowych z dostępem do Internetu. Niestety złośliwe oprogramowanie cyberprzestępcze jest liderem w tej technologii, a przemysł bezpieczeństwa złośliwego oprogramowania opóźnia się o trzy do sześciu miesięcy. Drugim frontem obronnym jest nasza świadomość istnienia fałszywych ofert internetowych i powstrzymywanie się od wpadania w pułapki cyberprzestępczości. Na przykład istnieją strony internetowe, które mają fantastyczne oferty produktów lub usług. Niektórzy obciążą Twoją kartę kredytową i nigdy nie dostarczą. W takim przypadku możesz ostrzec wystawcę karty kredytowej i spróbować uzyskać zwrot pieniędzy. Istnieją jednak inne oszukańcze witryny handlu elektronicznego, które po złożeniu zamówienia odpowiedzą, że takiego produktu nie ma na magazynie i że karta kredytowa nie zostanie obciążona. Rzeczywiście, Twoja karta kredytowa nie jest obciążana, ale dane uwierzytelniające karty są sprzedawane cyberprzestępcom. „Technologia może nas do tej pory zabrać, a resztą jest edukacja i czujność użytkowników komputerów". Istnieje wiele organizacji zajmujących się zwalczaniem cyberprzestępczości, a nasza świadomość ich istnienia jest ważna w naszej własnej

walce. Odpowiedzialność za popełnienie przestępstwa, czy to w świecie fizycznym, czy w cyberprzestrzeni, spoczywa na ramieniu ofiary. Na przykład, jeśli ktoś z fałszywą kartą oszuka bankomat i wykradnie pieniądze z konta, odpowiedzialność spoczywa na banku. Jeśli jednak ktoś korzystający ze schematu windykacji za pomocą naciśnięcia klawisza zhackuje Twoje kody bankowe i zaatakuje twoje konto, bank może odmówić „odpowiedzialności za stratę, ponieważ logowanie było autentyczne. Bank nie ponosi odpowiedzialności za integralność komputera klienta ”

Cyberprzestępczość w bankowości

Według różnych informacji prasowych setki banków są codziennie atakowane cybernetycznie, a łączne straty wynoszą prawie miliard dolarów. Tylko jeden bank azjatycki ukradł 101 mln USD, a odzyskano tylko 20 mln USD. Najwyraźniej działania te wymagały rozległych umiejętności w zakresie elektronicznego przesyłania funduszy, a także protokołów internetowych. Nawet niektóre amerykańskie banki były dysfunkcyjne z powodu cyberataków. Ponieważ niepraktyczne jest prowadzenie fizycznych przewodów lub dedykowanych łączy bezprzewodowych, od centralnego centrum IT banku do każdego bankomatu, banki używają sieci jako łącza komunikacyjnego z urządzeniami TM należącymi do kategorii Internetu rzeczy (IoT), z jego plusami i minusami. Wiele przedsiębiorstw, w tym banki, uważa, że cyberbezpieczeństwo można zwiększyć poprzez zakup większej ilości sprzętu. Jednak według urzędnika FBI: „Nie wystarczy budować ściany i hartować systemy, potrzebny jest kapitał ludzki, aby zrozumieć zagrożenie”. § Tam, gdzie ten kapitał ludzki, specjaliści ds. Bezpieczeństwa cybernetycznego, mają doświadczenie i wiedzę specjalistyczną oraz są na bieżąco na co dzień. Dla wszystkich przedsiębiorstw, w tym sektora bankowego, przeznaczanie milionów na bezpieczeństwo cybernetyczne jest nieuzasadnione, ale Royal Bank of Scotland nie wahał się podwoić swojego budżetu na bezpieczeństwo cybernetyczne do pół miliarda dolarów. Potrzeba cyberbezpieczeństwa jest podwójna: doświadczeni strategowie w pakiecie C i technicy w maszynowni IT.

Cyberprzestępczość w handlu elektronicznym

Praktycznie każda działalność komercyjna stara się wykorzystać korzyści płynące z Internetu, jednocześnie narażając się na cyberprzestępczość. Przepisy na całym świecie wyszczególniły cyberprzestępczość na ponad sto rodzajów i podlegały surowym karom, ale nie zniechęciło to przestępców do poszukiwania nielegalnych korzyści. Tak więc, według globalnych statystyk, wielkość handlu elektronicznego podwaja się rocznie. Walka z cyberprzestępczością stała się walką kooperacyjną z kupcami, rządem i konsumentem, której celem jest przynajmniej minimalizacja ta plaga. Osiągnięto konsensus co do środków zapobiegawczych, które muszą stosować konsumenci, które obejmują:

• Zachowaj system operacyjny komputera i zainstalowane aplikacje wszystko na bieżąco.

• Użyj najlepszej możliwej aplikacji antywirusowej. Nigdy nie polegaj na darmowych wersjach

• Używaj bezpiecznych sieci. Unikaj publicznych miejsc Wi-Fi, gdzie w tym samym obszarze fizycznym mogą znajdować się serwery obsługiwane przez cyberprzestępców.

• Kupuj przez zaufane strony internetowe. Cyberprzestępcy zakładają strony internetowe z „zaległymi okazjami”, aby uzyskać parametry karty kredytowej kupujących.

• Unikaj posiadania tego samego hasła do wielu krytycznych zastosowań. W związku z tym, jeśli zostanie naruszony, nie będzie działać na innych stronach internetowych.

• Unikaj wygody automatycznego wypełniania - szczególnie w przypadku finansów dane.

• Unikaj uwięzienia w grach internetowych, nagrodach, loteriach itp. Wiele takich publicznych stron internetowych jest zainfekowanych wirusem.

• Nie daj nikomu znać twoich haseł.

• Często zmieniaj hasła, w zależności od tego, jak ważny jest dostęp.

• Jeśli są dostępne, uczęszczaj na zajęcia uświadamiające na temat cyberbezpieczeństwa.

Cyberbezpieczeństwo na morzu

W dzisiejszej żegludze dostęp do Internetu jest tak samo, jak w dużym mieście. W ten sposób komunikacja online i w czasie rzeczywistym może odbywać się przez całą dobę. Za pomocą odpowiedniego Internetu Rzeczy (IoT) urządzenia centralne biuro może monitorować każdą aktywność na statku, taką jak

• Lokalizacja GPS

• Prędkość

• Skok i ziewanie

• Poziom paliwa

• Status zaciągów

• Zobacz kamery stacjonarne i mobilne na pokładzie

Podobnie jak w przypadku innych działań wspieranych przez cyberprzestrzeń, eksploatacja statku na środku oceanu wymaga morskich usług cybernetyki, które obejmują:

• Testy wytrzymałościowe i wytrzymałościowe

• Testy penetracji i segregacji sieci

• Skanowanie antywirusowe oraz łatki i aktualizacje oprogramowania

• Audyt uwierzytelnienia

• Bezpieczeństwo urządzeń przenośnych i IoT

• Ocena podatności

• Anomalie drogowe

• Monitorowanie urządzeń sieciowych

W kwestii bezpieczeństwa cybernetycznego na morzu Europejska Agencja Bezpieczeństwa Informacji o Sieci (ENISA) zaleca szkolenie uświadamiające na temat bezpieczeństwa cybernetycznego, które obejmuje wszystkich członków w dziedzinie morskiej, od sterników, operatorów terminali i żeglarzy, po głównych inżynierów i kapitanów