Meandry bezpieczeństwa danych

Cyberprzestępcy kierujący się zasadą tzw. nisko wiszących owoców zwykle zajmują się w pierwszej kolejności słabszymi systemami w bankach. Z drugiej strony instytucje finansowe muszą spełniać wymogi coraz bardziej prokonsumenckiego prawa. Czy technologie rzeczywiście zapobiegają utracie danych lub kradzieży ważnych informacji?

MAREK JAŚLAN

Sprawa zaczęła od jednego z klientów Sygma Banku, który wystąpił o zamianę posiadanej przez niego tzw. żółtej karty kredytowej jednego z supermarketów na kartę srebrną. Bank odmówił. W tej sytuacji zdenerwowany klient zażądał usunięcia swych danych z systemu informatycznego. Spór między bankiem a klientem na tyle się zaostrzył, że wmieszał się Generalny Inspektor Ochrony Danych Osobowych (GIODO). Bank ostatecznie usunął wszystkie dane klienta ze swego systemu. Pozostały one jedynie w elektronicznych kopiach zapasowych (tzw. backup) i są przechowywane w celach archiwalnych oraz dla bezpieczeństwa banku. Jednak GIODO nakazał usunięcie także kopii. Argumentował, że skoro nie było podstawy do wydania karty, to tym bardziej nie ma powodów do przechowywania danych klienta. Bank zaskarżył tę decyzję do sądu, argumentując, że przechowywanie danych w kopiach zapasowych nie narusza w żaden sposób interesu klienta, a z usunięciem danych z backupu mógłby mieć duży kłopot.

DANE Z OGRANICZENIAMI

Na początku tego roku Wojewódzki Sąd Administracyjny w Warszawie przyznał jednak rację GIODO i uznał, że banki powinny usuwać z kopii zapasowych dane swych byłych klientów. WSA uzasadnił, że praktyka banku narusza art. 26 ust. 1 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem administratorzy danych mają dopilnować m.in., aby dane były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Ten wyrok może zmusić banki do przebudowy systemów informatycznych i pokazuje, jak ważne przy tworzeniu systemów IT w bankach jest uwzględnianie przepisów prawa w zakresie danych osobowych.

Muszą o tym także pamiętać firmy informatyczne, które współpracują na tym polu z bankami.

– Rzeczywiście to wyjątkowy klient, bo regulacje prawne dotyczące instytucji finansowych w Polsce nakładają na nie wiele obowiązków zapewnienia bezpieczeństwa danych klientów i przeprowadzanych transakcji. Banki zobowiązane są do budowania specjalnych systemów kontroli dostępu do bankowych systemów IT – mówi Bartosz Stebnicki, dyrektor generalny EMC Poland, firmy oferującej informatyczne rozwiązania do zarządzania informacjami. Wyjaśnia, że takie systemy obejmują m.in. zapewnienie bezpieczeństwa fizycznego (kontrola dostępu do budynków) oraz uwierzytelniania użytkowników infrastruktury. Banki mają obowiązek budowania swoich systemów informatycznych w sposób, który zapewni ochronę danych i haseł umożliwiających ich przetwarzanie – zarówno przez klientów banku, jak i ich pracowników. Konieczne jest przy tym stałe monitorowanie funkcjonowania systemów informatycznych. Dodatkową komplikacją są przepisy nakładające na banki obowiązek zapisywania wszystkich zdarzeń zachodzących w ich systemach w sposób, który umożliwi ich kontrolę nawet po kilku latach.

O CZYM NALEŻY PAMIĘTAĆ, BUDUJĄC BEZPIECZNY SYSTEM INFORMATYCZNY?

Ważne jest:

- wydzielenie sieci komputerowych o zróżnicowanych stopniach „zmilitaryzowania",
- stosowanie urządzeń filtrujących ruch sieciowy (firewall),
- ścisłe zdefiniowanie zasad bezpieczeństwa i uprawnień zarówno w stosunku do poszczególnych modułów systemu, jak i do poszczególnych ról użytkowników,
- ścisłe zdefiniowanie zasad fizycznego dostępu do serwerów i innych kluczowych elementów systemu,
- odpowiednia organizacja monitorowania pracy systemu ze szczególnym uwzględnieniem procedur zapobiegania i wykrywania włamań,
- logowanie wszystkich dostępów do danych systemu,
- wprowadzenie procedur monitoringu operacji oraz możliwość przeprowadzenia dodatkowej weryfikacji.

PAMIĘTAĆ O PRZEPISACH

– Przy planowaniu systemów informatycznych w instytucjach finansowych koniecznie trzeba uwzględnić wiele serwisów technicznych nie realizujących funkcji stricte biznesowych, ale zapewniających ich bezpieczne, wydajne i ciągłe urzeczywistnianie – mówi Piotr Nogaś, menedżer w firmie Symantec Polska. Podkreśla on, że powinny one stanowić integralne rozwiązanie dostarczające niezbędne usługi z dziedziny ochrony danych (backup), wysokiej dostępności serwisów (rozwiązania klastrowe), bezpieczeństwa przetwarzania i kompleksowej kontroli dostępu, wydajności i zapewnienia ciągłości procesów biznesowych.

Przed wdrożeniem systemu informatycznego instytucje finansowe, które chcą stworzyć kompleksowy system ochrony danych, muszą najpierw opracować procedurę stałego obiegu dokumentów. Wymaga to opisania procesów zachodzących w firmie i procedur operacyjnych. – Kolejny krok polega na stopniowym usprawnianiu procesów, tak by stwarzały jak najmniej możliwości wycieku danych. Na tym etapie firmy sięgają po podstawowe rozwiązania IT – digitalizują dokumenty i automatyzują ich obieg. Oczywiście równolegle należy stosować technologie zabezpieczające firmę przed wirusami, atakiem z zewnątrz, takie jak systemy antywirusowe i firewall.

Instytucje finansowe, projektując swe systemy informatyczne, muszą zwracać uwagę na szczegółowe przepisy związane z ochro-

GŁÓWNE WARUNKI OCHRONY INFORMACJI

Najważniejszymi czynnikami dla ochrony informacji przetwarzanych w systemach i sieciach teleinformatycznych są:

- Prawidłowy dobór personelu – kryterium fachowości
- Specjalizacja – ochrona fizyczna, kryptograficzna, obieg wrażliwych informacji,
- Właściwe miejsce w strukturze organizacyjnej – bezpośrednia podległość kierownictwu
- Stałe wsparcie ze strony kierownictwa dla działań pionu bezpieczeństwa (co najmniej zrozumienie jego roli)
- Stałe podnoszenie i doskonalenie umiejętności – szkolenia organizowane dla personelu pionu bezpieczeństwa i przez personel pionu bezpieczeństwa
- Motywacja finansowa – albo nas stać na określony poziom bezpieczeństwa, albo wkalkulowujemy ryzyko związane z jego protezą.

ną danych o klientach, takie jak ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. Ale to zazwyczaj nie wystarcza. Procedury stosowane przez większość banków oraz systemy ochrony informacji pozwalają osiągnąć nawet wyższy stopień bezpieczeństwa danych osobowych niż wymagany w ramach wspominanej ustawy. To dlatego, że choć regulacje prawne określają główne zasady odnośnie utrzymania systemów informatycznych, to dobrą praktyką jest zabezpieczenie powyżej średniej. – Cyberprzestępcy kierujący się zasadą tzw. nisko wiszących owoców zwykle zajmują się w pierwszej kolejności systemami słabszymi – mówi Piotr Nogaś.

Technologia może jedynie ograniczyć ryzyko związane z utratą czy kradzieżą informacji. Można do tego dochodzić poprzez kompleksowe podejście do zabezpieczeń. Obejmuje ono wiele etapów, zaczynając od tego, na którym informacje i dokumenty są składowane – szyfrowanie dysków twardych podnosi bezpieczeństwo gromadzonych danych. Kolejne etapy, na których należy zabezpieczać informacje to: komunikacja między macierzami dyskowymi – między serwerami, między serwerami a aplikacjami, analiza zachowań użytkowników. Dodatkowo specyficzne typy informacji – takie jak ważne dokumenty, warto schować w repozytorium, co w praktyce oznacza przydzielenie praw do informacji (metadanych) i dokumentów określonym grupom pracowników, np. faktury mogą oglądać księgowi i zarząd, umowy jedynie dział inwestycji. Dalsze obniżenie ryzyka może przynieść użycie technologii zabezpieczającej dokumenty, niezależnie od ich miejsca położenia.

CZTERY KROKI PRZY SPORZĄDZENIU DOBREGO PLANU ZABEZPIECZEŃ

- Należy dokonać inspekcji wszystkich komputerów, jakie pracują w systemie informatycznym.
- Po dokonaniu inspekcji określić priorytety na podstawie prawdopodobieństwa wystąpienia problemu.
- Uwzględniając kolejno poszczególne zagrożenia, szeregując je według priorytetów, zdecydować, jak je odsunąć, złagodzić lub jak ich unikać (albo zastanowić się, czy można pracować mimo istnienia tych zagrożeń).
- Utworzyć zespół, przydzielić zasoby i obowiązki, a następnie zrealizować plan. Pamiętać o ciągłej weryfikacji i nadzorowaniu przestrzegania planu.

NIEPEWNY OUTSOURCER?

Wiele banków ma obawy, czy powierzanie swych systemów informatycznych i danych tam zgromadzonych firmom outsourcingowym jest bezpieczne. Często pada pytanie, do którego momentu odpowiedzialność za sprawność systemu ponosi outsourcer, a kiedy spoczywa ona na użytkownikach, którzy, jak pokazuje praktyka, są sprawcami sporej części problemów nękających firmowe IT. Klient ma prawo wymagać od outsourcera zapewnienia bezpieczeństwa technicznego, psychologicznego i prawnego. Bezpieczeństwo techniczne gwarantują centra przetwarzania danych (data center) – profesjonalne serwerownie odpowiednio fizycznie zabezpieczone zarówno przed dostępem osób niepowołanych, jak i przed zdarzeniami losowymi – pożarami czy powodzią. Na straży danych naszych klientów stoją specjalne procedury, obejmujące monitorowanie obiektu, alarmy antywłamaniowe i pożarowe oraz elektroniczną kontrolę dostępu. Odnośnie bezpieczeństwa psychologicznego – klienci często niepokoją się o dostęp do danych osób niepowołanych, zapominając o tym, że pracownicy outsourcera, w przeciwieństwie do własnych, nie są w stanie wskazać strategicznych informacji. Dlatego outsourcer w umowie powinien dać gwarancję dostępności systemu i zobowiązać się płacić odszkodowania w przypadku niedotrzymania warunków umowy. Trzeba też pamiętać, że własny pracownik niewiele ryzykuje, sprzedając informacje – zaś obecność firmy outsourcingowej na rynku jest pochodną kredytu zaufania klientów. Dlatego firmy outsourcingowe niezwykle starannie dobierają pracowników i nierzadko opracowują w tym celu specjalne wewnętrzne procedury. Z kolei w kwestiach prawnych jest szczególnie ważne, żeby ustalić wzajemną odpowiedzialność, a także sposób komunikacji i raportowania podczas całego precyzyjnie określonego czasu trwania umowy. W przypadku nieprzewidzianych zdarzeń klient powinien otrzymać gwarancję odtworzenia systemu w przewidzianym umową terminie, może też dochodzić odszkodowania za poniesione straty.

NAJNIEBEZPIECZNIEJSZY WŁASNY PRACOWNIK!

Nawet szefowie firm informatycznych nie próbują jednak przekonywać, że da się zbudować system informatyczny w 100 proc. nie do przejścia. Podstawową zasadą przy budowaniu systemu bezpieczeństwa w firmie jest uznanie, że nie ma cudownego środka, który całkowicie wyeliminuje zagrożenia. Nawet jeśli wdrożymy dostępne na rynku technologie zabezpieczające, nie mamy gwarancji, że ktoś nie skopiuje danych, na przykład używając aparatu fotograficznego wbudowanego w telefon. – Na system bowiem składa się zarówno sprzęt, jak i oprogramowanie, a nie ma programu bez błędów, są tylko takie, w których jeszcze nie wykryto wszystkich uchybień – mówi Andrzej Marcol, dyrektor ds. rozwoju technologii w firmie Archidoc. Częste wpadki bywają bardzo dotkliwe. Przykład mieliśmy okazję zaobserwować w styczniu, kiedy przydarzyła się wpadka centrum rozliczeniowemu Visa, które przekazało do banków błędne dane o transakcjach kartowych.

CO MOŻE GROZIĆ NASZEJ INSTYTUCJI?

- Zdarzenia losowe – awarie sieci energetycznej, pożary, klęski żywiołowe
- Niezamierzony błąd człowieka – skasowanie ważnych danych, wysłanie ważnych informacji do niewłaściwego adresata, uruchomienie wirusa
- Celowe działanie na szkodę firmy (od wewnątrz – ze strony nieuczciwego pracownika, jak i z zewnątrz) – skasowanie ważnych danych, nieautoryzowany dostęp do systemu informatycznego, atak hakerów

CO ZROBIĆ, ŻEBY PRACOWNIK NIE UKRADŁ DANYCH?

Konieczne jest:

- ścisłe zdefiniowanie uprawnień na poszczególnych stanowiskach pracy,
- logowanie informacji o udostępnieniu określonych danych konkretnym osobom,
- budowanie świadomości pracowników o istnieniu tych logów i o możliwości dotarcia do potencjalnych źródeł ewentualnego wycieku,
- zawarcie w procedurach bezpieczeństwa mechanizmów kontroli ich przestrzegania,
- częste przypominanie pracownikom o obowiązujących zasadach bezpieczeństwa i kontrole ich stosowania.

Najprawdopodobniej zawiodło oprogramowanie, które w jakiejś szczególnej, nieprzewidzianej sytuacji zadziałało niepoprawnie. Luki w systemie informatycznym powodują, że bank może ponieść dwa rodzaje szkód. Pierwsze te bezpośrednie straty materialne, związane z uszkodzeniem zasobów teleinformatycznych, koniecznością ich odtworzenia i – co jest z tym związane – niemożnością świadczenia usług drogą elektroniczną. Drugi rodzaj to straty pośrednie, takie jak negatywny wpływ na wizerunek i wiarygodność instytucji finansowej. Nic więc dziwnego, że poszkodowane instytucje zwykle nie chcą upubliczniać informacji w obawie przed utratą klientów. Dlatego, projektując system IT w banku, warto zdać sobie sprawę, skąd płynie największe zagrożenie.

Dzisiaj raczej nie zdarzają się włamania do systemów bankowych skutkujące przejęciem nad nimi kontroli przez włamywaczy. Zabezpieczenia typu „firewall" oraz bieżący monitoring są w stanie wcześnie wykryć próby włamania do systemu. Bardziej niebezpieczne są usiłowania wykradania informacji poprzez podszywanie się przestępców pod pracowników banku bądź preparowanie stron internetowych do złudzenia przypominających strony bankowe, czyli phishing. Specjaliści twierdzą, że najgroźniejsze jest wykradanie poufnych danych, takich jak loginy, hasła, numery kart kredytowych. Metodą obrony przed takimi atakami są: określenie ścisłych procedur, a przede wszystkim informowanie klientów o tych procedurach i uczulenie ich, że jakiekolwiek odstępstwo powinno być traktowane jako potencjalne zagrożenie.

Wielkie zagrożenie dla systemów informatycznych instytucji finansowych stanowią ataki dokonywane przez pracowników placówek wewnątrz sieci. Systemy zabezpieczenia danych stosowane przez banki są stale doskonalone, podlegając rygorystycznym przepisom i procedurom. Jednak nie są one w stanie wyeliminować zagrożenia płynącego z niefrasobliwego czy też niezgodnego z prawem działania pracowników. Wykorzystując uprawniony dostęp do systemów, mają oni możliwość dokonania wielu nadużyć, takich jak: wyprowadzenie danych na zewnątrz poprzez e-mail czy skopiowanie do pamięci USB, umyślne lub nieumyślne wprowadzenie do systemu niepożądanego oprogramowania (konie trojańskie) służącego kradzieży danych. Generalnie jednak klienci polskich banków mogą spać spokojnie, bo procedury wewnętrzne oraz systemy kontroli dostępu do danych pozwalają bankom w porę wykryć i udaremnić niebezpieczne zachowania.

Chcąc zabezpieczyć się przed takimi przypadkami, instytucje finansowe inwestują np. w rozwiązania klasy DLP (data loss prevention) pozwalające klasyfikować i chronić dane przed wyciekiem oraz tworzyć systemy chroniące przed kradzieżą danych zarówno na poziomie centrów przetwarzania danych, w sieci korporacyjnej, jak i ze stacji roboczych. Klasyfikacja dokumentów odbywa się automatycznie – system dokonuje analizy zawartości plików pod kątem wystąpienia słów kluczowych, charakterystycznych fraz czy też zgrupowań liczb. Wyciek sklasyfikowanych danych jest uniemożliwiany m.in. poprzez blokowanie kopiowania czy wydruku dokumentów.

Rynek systemów ochrony danych w Polsce rozwija się w podobnym stopniu jak w Europie Zachodniej i USA. I z dumą możemy stwierdzić, że poziom zabezpieczeń bankowości elektronicznej w Polsce jest wyższy niż w niektórych krajach Europy Zachodniej

Autor jest dziennikarzem dziennika „Polska" specjalizującym się w tematyce informatycznej