

+ Złap mnie jeśli potrafisz

Redundancja zwiększa możliwość kradzieży danych przez pracowników, jednak niewiele firm wystarczająco się tym przejmuje i lub w ogóle wierzy w taką możliwość.

Sprawa bezpieczeństwa informatycznego w firmach często przypomina sytuację niezależnego państwa. Pracownicy są elektoratem (i mają mniej więcej tyle samo do powiedzenia) kierownicy poszczególnych działów przypominają wojewodów a CEO to El Presidente. To czyni z CIO mieszankę zastępcy prezydenta i szefa wywiadu – on lub ona jest odpowiedzialna zarówno za codzienne życie organizacji jednocześnie wypatrując potencjalnych zagrożeń z zewnątrz. Niestety zbyt wielu CEO patrzy na bezpieczeństwo IT jak na straż graniczną – sprowadza się do wypatrywania wrogów na odległym horyzoncie. W rzeczywistości, znaczna część zagrożeń pochodzi z samego wnętrza organizacji i nie jest zaskakujące, że to nie technologii powinni się najbardziej obawiać. Podczas gdy systemy mogą zostać polatane i zabezpieczone, oraz wymagające autentykacji, największe zagrożenie ochrony danych pochodzi od samych użytkowników, których motywować może np. zemsta lub zwyczajnie korzyści majątkowe. Ochrona tych danych przed tymi ludźmi, którzy akurat powinni mieć do niej dostęp przyprawia menadżerów IT o potworny ból głowy.

Oczywiście wielu nie wierzy w istnienie takiego zagrożenia. I w tym tkwi problem – w przeciwieństwie do Europy Zachodniej czy Stanów Zjednoczonych gdzie firmy muszą ujawniać incydenty wycieku danych, u nas niema podobnych wymogów. Przez to firmy wpadają w stan uśpionej czujności i poczucia bezpieczeństwa. Specjaliści od bezpieczeństwa danych potwierdzają, że wycieki są codziennością: „Jest wiele powodów, dla których nie słyszymy często o tych incydentach, przede wszystkim związanych z potencjalną szkodą dla reputacji czy marki firmy”. „Drugim ważnym powodem dlaczego nie trafiają one do publicznej wiadomości jest fakt, że zarządzanie i widzialność takich informacji nie należy do domeny publicznej. Teraz jednak wraz ze wzrostem zainteresowania przejrzystością takich spraw, staną się one bardziej dostępne dla środowisk komercyjnych i publicznych”. W rzeczywistości, wiele firm przygląda się bezpieczeństwu danych dopiero po fakcie. Problemem jest zbyt częste oparcie bezpieczeństwa danych o zaufanie. „Widzimy, że to się dzieje. Może to zostać utrzymane w tajemnicy przed zewnętrznym światem”. Firmy dowiadujące się o wyciekach coraz częściej szukają rozwiązań. Zdaniem niektórych, taki stan rzeczy to kolejny efekt uboczny kryzysu. „Zwłaszcza w czasie recesji, wielu pracowników zostało pozbawionych pracy. Ciężko dla nich jest znaleźć miejsce na rynku. Dla wielu pracowników to szansa jak na loterii, zwłaszcza sekcjach bezpieczeństwa informatycznego. Jedną z najgorszych pułapek jest fakt, że kiedy ludzie ci odchodzą z firmy, zabierają ze sobą prawa autorskie. Wiele organizacji mówi, że kiedy ktoś od nich odchodzi zabiera ze sobą dane”.

Ważna jest klasyfikacja informacji w obrębie organizacji, tworzenie świadomości u pracowników jakie są konsekwencje wycieku danych i jak powinni reagować. W większości przypadków, tylko pierwsza połowa przekazu zostaje przyswojona. Pracownicy dowiadują się, że dane są poufne, nie mówi się im jak powinni się wobec tego zachować. Czy powinni przestać z nich korzystać?

Innym problemem jest nie jasność polityk bezpieczeństwa odnośnie informowania pracowników, że dane, z których na co dzień korzystają w pracy nie należą do nich. „Nawet pomimo, że dane są zbierane podczas ich pracy, prawo własności w 100% należy do firmy. Nie jest to takie oczywiste dla pracowników nie tylko u nas ale i na całym świecie. Wysoki priorytet zyskuje w firmach wytworzenie świadomości i informowanie pracowników o tym do kogo należą dane i jakie są procedury”.



Niestety dla menadżerów bezpieczeństwa IT, praktycznie każde urządzenie z którym pracownik wejdzie w kontakt podczas swojego dnia pracy staje się potencjalnym narzędziem przecieku, nieraz nawet niezamierzonym. Od pamięci przenośnej po nieograniczony dostęp do maila, okazji do wycieku danych może być wiele. Problem jest złożony, szczególnie przy obecnym trendzie korzystania z PDA i laptopów, odzwierciedlającym zwiększenie mobilności siły roboczej. Chociaż łatwo jest wyobrazić sobie jak mogłyby zostać użyte do wyniesienia danych, to jest jeszcze inna strona ignorowana przez firmy.

„Dzisiaj większość laptopów i serwerów używanych w firmie jest zarządzana przez dostawców. W większości przypadków kiedy następuje potrzeba wymiany komponentów kwestie bezpieczeństwa schodzą na dalszy plan. Urządzenie lub serwer wychodzi z użycia ale dane nadal na nim pozostają. Najczęściej można to zauważyć u klientów – wysyłają laptopy do przeglądu nie szyfrując danych. Osoba naprawiająca urządzenie ma łatwy dostęp do tych danych. Ludziom wydaje się, że jeśli umieszczą hasło to będzie to wystarczające, ale w rzeczywistości tak nie jest. Zawsze można podłączyć twardy dysk do innego urządzenia i pobrać wszystkie dane”.

W teorii, pracownicy są kierowani polityką ustanowioną przez dział kadr, zabraniającą traktowania danych w niestosowny sposób. Ciężko jest chronić dane przepisami znajdującymi się jedynie na papierze.

„Jedyną rzeczą jaką mamy jest nasza polityka, ta na piśmie. Pozostawiona jest ona uznaniu pracowników, czy zamierzają się do niej stosować, czy nie”. Na przykład, jeśli przepisy mówią, że dysk USB są używane do transportu danych a ludzie się do tego stosują to można uznać, że wszystko gra. Ale jeśli porty USB są otwarte na naszym komputerze, wówczas każdy pracownik może coś do nich podłączyć i skopiować dane. Jeśli odejdziesz z firmy i zechcesz przekazać komuś dane to nie będzie miało znaczenia jaka polityka została spisana. Ważniejsze dla firm z poufnymi danymi jest skuteczne uniemożliwienie wynoszenia krytycznych danych na zewnątrz.”

Problem leży w tendencji do planowania polityk przez firmy ale nie w utrzymywaniu ich:

„Firmy zaczynają od dobrych chęci tworząc przepisy i procedury lecz

+ Złap mnie jeśli potrafisz

nie sprawdzając ich regularnie.

To co dzieje się po drodze to niechęć decydentów do ciągłego wydawania pieniędzy na wspieranie i przeprowadzanie oraz ponowne pisanie przepisów, a także edukacja pracowników czy przeprowadzanie audytów."

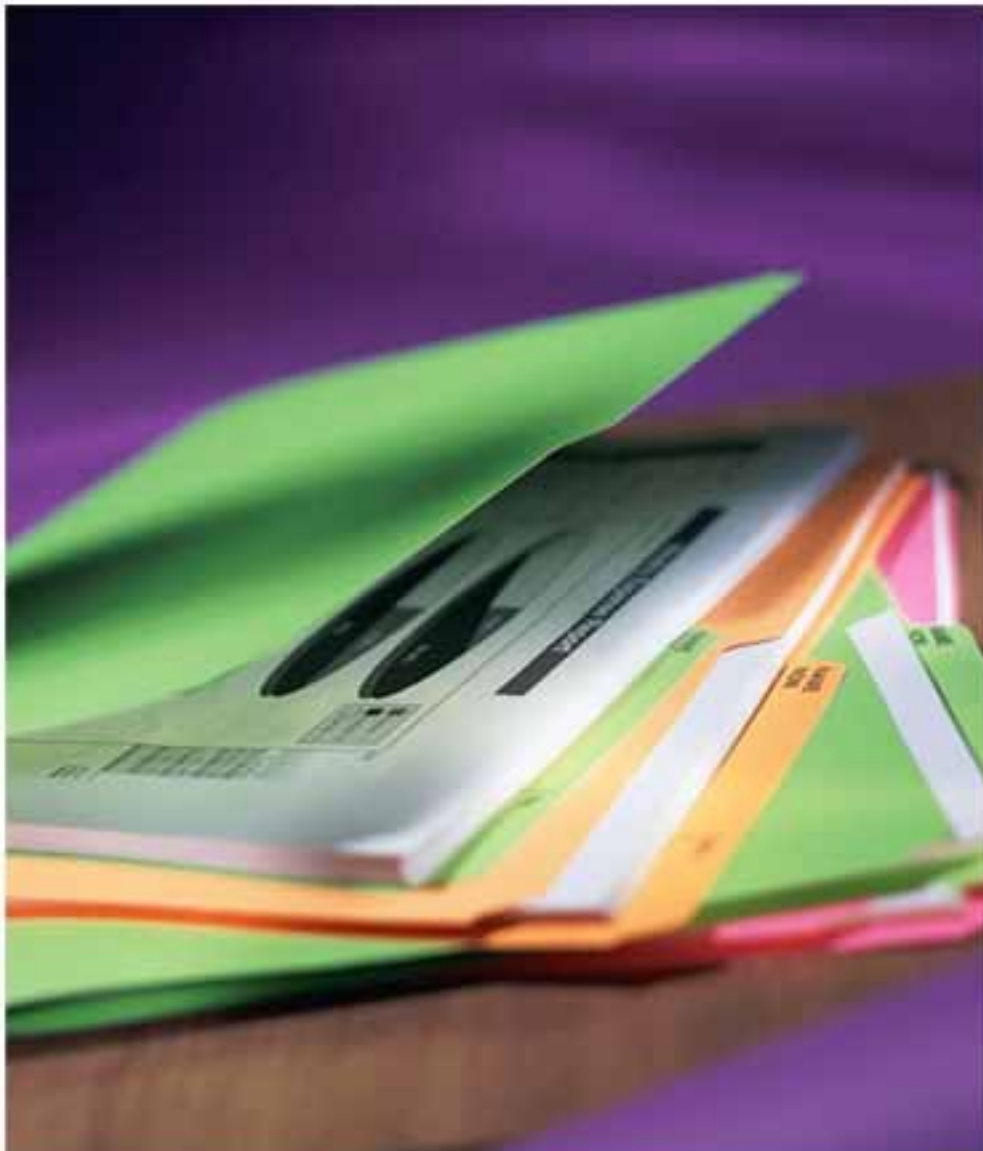
Zdaniem wielu tworzenie polityk i wdrażanie ich powinno pozostać domeną kadr: „Zalóżmy, że wdrożenie odbywa się z udziałem kadr i działu bezpieczeństwa. W rezultacie jeśli pracownik dokona jakiegoś naruszenia przepisów mającego silne konsekwencje to naruszenie musi być wsparte przez przepisy kadr. Jeśli spojrzeć na podręczniki bezpieczeństwa w firmach to widać że są własnością działu kadr."

Jednak wiedzę pracowników o kwestiach HR nie należy brać za pewniak.

„Często pracownicy robią rzeczy nieświadomie. Jest bardzo ważne aby firmy i szefowie przekazywali jasną wiadomość, że informacje używane przez nas na co dzień mają charakter poufny. Ważna jest klasyfikacja informacji w obrębie organizacji, tworzenie świadomości u pracowników jakie są konsekwencje wycieku danych i jak powinni reagować. W większości przypadków, tylko pierwsza połowa przekazu zostaje przyswojona. Pracownicy dowiadują się, że dane są poufne, nie mówi się im jak powinni się wobec tego zachować. Czy powinni przestać z nich korzystać?"

Należy pamiętać, że pracownicy działu IT nie znajdują się poza regulacjami działu kadr. Największym koszmarem wielu organizacji jest niezadowolony pracownik IT mogący wyrządzić poważne szkody. Jedynym zabezpieczeniem na taką ewentualność jest dokonywanie ciągłych audytów.

„Nie tylko audytujemy dział IT, ale audytujemy również administratorów systemów i przełożonych oraz osoby stojące ponad nimi. Jednymi z największych naruszeń wymogów bezpieczeństwa są przypadki dokonane przez ekspertów. Np. pracownicy działu IT, stają się niezadowoleni i odchodzą z danymi. Potrzeba pełnego śladu od sponsora danych, przez obróbkę danych po właściciela firmy.



Jeśli dane znikną, to firma wie co robi dział IT, dział IT wie co robią jego pracownicy a osoba odpowiedzialna za wyciek, która może być nawet administrator systemu jest również poddawana audytowi.

„Jeśli spojrzeć na większość organizacji, audytorzy są często powiązani z działem IT. To nie jest dobry pomysł. W obecnym scenariuszu to przesuwanie planowania ciągłości biznesu i bezpieczeństwa z działu IT i raportowanie bezpośrednio do CIO. Dzięki czemu rola dedykowanego administratora bezpieczeństwa jest ważniejsza niż kiedykolwiek. Są jak niewidzialni bohaterowie. W momencie kiedy pracownik odchodzi z firmy, jest odpytywany do jakich danych posiadał dostęp, aby dane natychmiast zostały mu odebrane, a dostęp zamknięty. " Kluczowe jest sprawdzanie historii pracownika: „Ważne jest filtrowanie administratorów w momencie przyjmowania do pracy. Niestety kiedy dajemy im dostęp to powinniśmy zdawać sobie sprawę, że administrator będzie miał dostęp praktycznie do wszystkiego. Trzeba być bardzo ostrożnym przy doborze tych ludzi, aby wybrać tych, którym możemy zaufać."

Ściganie to kolejny trudny temat, zwłaszcza tam gdzie prawa związane z wyciekami danych są niewystarczające. Najlepszą praktyką jest podwójne zabezpieczenie polegające na zobowiązaniu podpisanego przez pracownika i stosowaniu odpowiednich przepisów.

„Większość firm jako metodę prewencyjną stosuje umowy o tajemnicy danych podpisywane przez pracowników (NDA). Kiedy trzeba ścigać pracownika, który naruszył NDA, ciągle można napotkać wiele problemów, szczególnie tam gdzie wielu pracowników to expatrianci z innych krajów. Zależy to również od rodzaju dwustronnych umów jakie istnieją pomiędzy oboma krajami."

Ważne jest filtrowanie administratorów w momencie przyjmowania do pracy. Niestety kiedy dajemy im dostęp to powinniśmy zdawać sobie sprawę, że administrator będzie miał dostęp praktycznie do wszystkiego. Trzeba być bardzo ostrożnym przy doborze tych ludzi, aby wybrać tych, którym możemy zaufać.

„Kraje zdają sobie sprawę z wagi bezpieczeństwa danych i stosują różne prawa. Jeśli udamy się do DIFC, to zobaczymy, że mają własne przepisy bezpieczeństwa zapewniające, że wykorzystywane dane są chronione według międzynarodowych standardów."

Ostatecznie jednak niemożliwe przewidzenie kiedy pracownik postanowi nam zaszkodzić, pewne jest jednak to, że im wyżej dany pracownik stoi w hierarchii tym dotkliwsze będą szkody. Zadaniem CIO jest równowaga między zapewnieniem bezpieczeństwa w firmie, a nie stosowanie przesadnych rygorów, które jak w sam raz mogą dać powód do niezadowolenia i stać się lekarstwem gorszym od choroby. Należy również oczywiście upewnić się czy kadra zarządzająca rozumie zagrożenie wynikające z dawania zbyt dużej swobody pracownikom.

P.P.