Wprowadzenie do koncepcji zasad bezpieczeństwa

Polityka bezpieczeństwa (lub polityka bezpieczeństwa informacji) to dokumentacja określająca wymagania operacyjne, procedury i ograniczenia, których należy przestrzegać, zanim organizacja będzie mogła zostać uznana za bezpieczną. Polityka wyjaśnia również pracownikom, czego się od nich oczekuje, a ponieważ przestrzeganie polityki bezpieczeństwa powinno być częścią warunków zatrudnienia, zapewnia ramy dyscyplinarne w przypadku zignorowania tej polityki. Jednak dobrze napisana i wykonana polityka to znacznie więcej niż zwykły kij do pokonania pracowników (chociaż wiele firm, ignorujących podstawowe bezpieczeństwo operacyjne, uważa to za nic innego). To narzędzie zwiększające bezpieczeństwo organizacji na każdym poziomie:

• Definiuje operacyjne procedury bezpieczeństwa (kroki, które należy podjąć podczas sprawdzania pracowników, minimalna długość hasło i tak dalej);

• Zapewnia, że pracownicy są świadomi tego, czego się od nich oczekuje (w zakresie postępowania z poufnymi informacjami, nie zapisywania haseł itd.);

• Przedstawia kroki, które należy podjąć w przypadku wystąpienia zdarzenia naruszającego bezpieczeństwo. Zauważysz, że te cele się pokrywają; jest to zarówno zamierzone, jak i nieuniknione.

Ta część skupia się na aspektach, które należy wziąć pod uwagę podczas tworzenia dokumentacji polityki bezpieczeństwa. Ponieważ praktycznie każdy aspekt biznesu można w jakiś sposób uregulować, ten rozdział koncentruje się na najważniejszych obszarach (przynajmniej z punktu widzenia tej książki), więc nie będę zwracał zbytniej uwagi na takie rzeczy jak antywirus i łatka oprogramowanie do zarządzania. Korzyści płynące z takich technologii powinny być oczywiste dla każdego, kto czyta tę książkę, co nie oznacza, że nie powinny być objęte polityką. Chcę tylko, żeby było bardziej interesujące i istotne. W tym rozdziale przeanalizowano następujące aspekty bezpieczeństwa i podano przykłady ich regulacji:

• Bezpieczeństwo fizyczne i kontrola dostępu;

• Materiał zabezpieczony lub sklasyfikowany;

• Bezpieczeństwo komunikacji;

• Weryfikacja przeszłości;

• Bezpieczne niszczenie danych;

• Szyfrowanie danych;

• Outsourcing;

• Reagowania na incydenty.

Obszary te są najbardziej istotne z punktu widzenia głównego tematu i pod koniec rozdziału powinno być jasne, w jaki sposób ich łagodzenie i dokumentowanie mogłoby zapobiec lub przynajmniej udaremnić wiele omówionych ataków. Każda sekcja tutaj z łatwością wypełniłaby własną książkę; są to odrębne dyscypliny i obszary specjalizacji same w sobie. Bardzo trudno jest zaplanować środki bezpieczeństwa bez dobrej polityki i praktycznie niemożliwe jest oszacowanie Twojej ciągłej zdolności do odparcia ataku. Dlatego tam, gdzie to możliwe, załączam przykłady zasad bezpieczeństwa, które możesz ponownie wykorzystać we własnej dokumentacji.

Bezpieczeństwo fizyczne

W tej części zasad bezpieczeństwa opisano fizyczne zagrożenia, które są związane z twarzami organizacji, środkami zastosowanymi w celu jej ochrony i konkretne wytyczne dotyczące wdrażania. W kontekście bezpieczeństwa informacji celem jest ochrona systemów informatycznych przed atakiem i włamaniem. Można to osiągnąć na wiele sposobów, a proste przykłady obejmują wymóg zamykania drzwi lub określenie konkretnej marki zamka o wysokim poziomie bezpieczeństwa, który ma być używany. Bezpieczeństwo fizyczne można opisać tak szczegółowo, jak chcesz, ale zwykle obejmuje następujące obszary:

• Bezpieczeństwo obwodowe;

• Kamery i telewizja przemysłowa;

• Kontrola dostępu;

• Ludzkie bezpieczeństwo;

• Fizyczne bezpieczeństwo poczty;

Ponownie, lista ta nie jest ostateczna i zawiera pokrywające się tematy.

Bezpieczeństwo graniczne

Bezpieczeństwo graniczne gwarantuje, że fizyczne granice witryny są bezpieczne. Sposób, w jaki jest to realizowane w praktyce, zależy od charakteru terenu, aktywów wymagających ochrony i postrzeganego poziomu zagrożenia. Na przykład fabryka papieru prawdopodobnie nie potrzebuje 3-metrowych ścian z drutem ostrzowym i czujnikami ruchu, ale w przypadku więzienia byłoby to absolutne minimum. Funkcją bezpieczeństwa granicy jest zapewnienie fizycznego i prawnego środka odstraszającego przed wtargnięciem oraz zapewnienie jasnej, prawnie wykonalnej granicy. Przykłady zasad, które dotyczą bezpieczeństwa granic, obejmują:

• Ogrodzenie obwodowe powinno mieć nie mniej niż metry wysokości i ze swej natury powinno wskazywać granicę terenu prywatnego.

• Oświetlenie obwodowe powinno zapewniać dostateczne oświetlenie wewnątrz i wokół obiektów, aby wykrywać i obserwować zbliżających się ludzi. Powinno to zniechęcać do włamań i oportunistycznych działań przestępczych, takich jak kradzież lub wandalizm.

• Obwód obiektu powinien być wyraźnie oznaczony, na przykład za pomocą znaków zewnętrznych. Znaki powinny być umieszczone tak, aby były dobrze widoczne ze wszystkich stron obiektu.

• Kształtowanie krajobrazu powinno wspierać ochronę obiektów i mienia poprzez promowanie nadzoru i minimalizowanie osłony dostępnej dla intruza. Obwód, szczególnie w punktach wejścia i wyjścia, powinien być objęty monitoringiem CCTV. Urządzenia CCTV powinny mieć nawzajem wyraźne pole widzenia.

Monitoring telewizji przemysłowej

Większość obiektów wykorzystuje przynajmniej ograniczone zabezpieczenia kamery i powinno to być określone w polityce bezpieczeństwa, aby zapewnić prawidłowe planowanie i wdrożenie operacyjne. Zasady powinny określać, jakie są kamery umieszczone i monitorowane oraz jak pracownicy ochrony reagują na podejrzewany incydent. Dobrze rozmieszczone systemy CCTV są nieocenione w ochronie fizycznego bezpieczeństwa obiektu, chociaż nigdy nie można na nich całkowicie polegać, jak już widzieliście. Telewizja przemysłowa zapewnia połączenie odstraszania, monitorowania i prawnego

niezaprzeczalności. Poniżej znajdują się ogólne przykłady instrukcji, które należy uwzględnić w polityce bezpieczeństwa, które mogą zostać dostosowane przez dowolną organizację:

• Wszystkie obszary lokalu powinny być objęte CCTV, o ile jest to wykonalne, ze szczególnym uwzględnieniem punktów wejścia i wyjścia, wind i wejścia do obszarów chronionych.

• Obszary bezpieczne powinny być objęte systemem telewizji przemysłowej na żywo w czasie, gdy jest do nich możliwy dostęp.

• Cały personel monitorujący CCTV powinien być certyfikowany na odpowiednim poziomie, po ukończeniu kursu, który uczy wszystkich niezbędnych operacyjnych i prawnych aspektów pracy.

• Jakość obrazów CCTV musi być dostatecznie wysoka, aby można je było złożyć jako dowód w sądzie.

• Kamery CCTV muszą być zdolne do ciągłej pracy w środowisku, w którym są rozmieszczone. W zmieniających się warunkach (na przykład przy słabym oświetleniu) kamery powinny mieć zadowalające możliwości noktowizyjne lub termowizyjne.

Kontrola dostępu

W bezpieczeństwie informacji, biorąc pod uwagę wystarczająco szeroki kontekst, kontrolę dostępu można rozszerzyć tak, aby oznaczała praktycznie wszystko. W przypadku bezpieczeństwa fizycznego odnosi się w szczególności do przywilejów dostępu przyznanych personelowi i gościom oraz sposobu ich egzekwowania. Obejmuje to zasady dotyczące plakietek i przepustek identyfikacyjnych, sposób obsługi odwiedzających, technologię używaną do oddzielania przywilejów w budynku (np. Tokeny elektroniczne) oraz rodzaje barier, które należy przekroczyć, aby uzyskać dostęp do budynku lub bezpiecznego obszaru, np. pułapki na ludzi. Ze względu na stale zmieniające się oblicze technologii dobrym pomysłem jest utrzymywanie oświadczeń politycznych w odniesieniu do konkretnych środków, które są dość niejasne, ale jednocześnie wystarczająco szczegółowe, aby nie pozostawiać żadnych operacyjnych błędnych interpretacji. Poniższy zakres oświadczeń dotyczących zasad jest dobrymi przykładami tego, o czym należy pomyśleć:

• Wszyscy pracownicy, wykonawcy i goście są zobowiązani do noszenia oficjalnych identyfikatorów przez cały czas. Każdy, kto nie ma oficjalnej identyfikatora powinien być wyzwaniem.

• Żetony zbliżeniowe są wymagane do otwierania drzwi odpowiednich do poziomu dostępu posiadacza.

• Do obszarów, do których wprowadzono żetony zbliżeniowe (lub inną kontrolę elektroniczną), może wejść tylko posiadacz tokena. Żetonów nie wolno udostępniać innym członkom personelu, gościom ani kontrahentom. Jednakże członkowie personelu mogą otwierać drzwi dla gości, za których są bezpośrednio odpowiedzialni, pod warunkiem, że goście są eskortowani.

• Zabrania się zezwalania innym osobom na dostęp do obszarów dostępnych za pomocą żetonów zbliżeniowych. Jeżeli ktoś, kto nie posiada ważnego tokena, wkroczył do bezpiecznego obszaru, powinien zostać zakwestionowany.

• Zgubiony lub skradziony identyfikator lub token zbliżeniowy należy niezwłocznie zgłosić do działu bezpieczeństwa.

• Wszyscy odwiedzający muszą zarejestrować się w recepcji, gdzie otrzymają tymczasowe identyfikatory. Odwiedzający muszą pozostać w recepcji w oczekiwaniu na punkt kontaktowy.

• Wszyscy odwiedzający mogą zostać poddani przeszukaniu w dowolnym momencie.

• Wszyscy goście muszą być eskortowani przez pełnoprawnego pracownika (nie wykonawcę) na czas ich pobytu.

Ludzkie bezpieczeństwo

Użyłem terminu „bezpieczeństwo ludzi" z braku czegoś lepszego („polityka inżynierii antyspołeczneja" po prostu brzmi głupio). Wiesz już , jakiego rodzaju zagrożeniom należy przeciwdziałać. Oznacza to edukację personelu i uczynienie świadomości bezpieczeństwa priorytetem, ale pewne zachowania i reakcje powinny być podyktowane polityką bezpieczeństwa: w ten sposób zasady obowiązują wszystkich i nikt nie może narzekać, że są niesprawiedliwie traktowani. Nie jest możliwe wyszkolenie personelu w celu ciągłego wykrywania ataku, co nie jest pożądane. Jeśli staniesz się zbyt paranoikiem, po prostu robienie interesów staje się niemożliwe. Staraj się osiągnąć równowagę w kwestiach bezpieczeństwa ludzi. Poniżej przedstawiono sugerowane stwierdzenia, które można włączyć do polityki bezpieczeństwa:

• Jeśli to możliwe, pracownicy powinni unikać omawiania informacji poufnych przez telefon. Pracownicy nigdy nie powinni omawiać ani przekazywać informacji poufnych lub zastrzeżonych komuś, kogo nie znają, niezależnie od tego, za kogo się podają. Jeśli rozmówca jest zdenerwowany lub zły, natychmiast przekaż go swojemu przełożonemu.

• Pracownicy powinni dokładnie sprawdzić adresy e-mail lub podpisy szyfrowania przed odpowiedzią na wiadomość e-mail dotyczącą informacji wrażliwych lub uprzywilejowanych. W razie wątpliwości nie odpowiadaj.

• Pracownicy nigdy nie powinni otwierać załączników do wiadomości e-mail od nieznajomych. Pracownicy powinni powstrzymać się od wysyłania plików pocztą elektroniczną, gdy tylko jest to możliwe, i zamiast tego powinni korzystać z bezpiecznych zasobów wewnętrznych.

• Pracownicy powinni być świadomi swojego otoczenia. Osoby zachowujące się podejrzanie powinny zostać wezwane lub zgłoszone do ochrony.

Fizyczne bezpieczeństwo poczty

Kiedy Unabomber został złapany, świat korporacji odetchnął z ulgą. Strach przed otrzymaniem bomb z gwoździami i innych nieprzyjemnych niespodzianek pocztą wydawał się już przeszłością. Wszystko zmieniło się po 11 września i atakach wąglika, które ogarnęły Stany Zjednoczone. W Wielkiej Brytanii w 2007 r. wiele urządzeń zostało wysłanych na adresy firmowe, w tym do Agencji ds. Licencji Kierowców i Pojazdów (DVLA). Korzystanie z usług pocztowych w celu dostarczania wybuchowych i trujących paczek do celów jest powszechną taktyką różnych grup i zadaniem każdego jest złagodzenie niebezpieczeństwa, jakie to stanowi. W związku z tym nie jest złym pomysłem przynajmniej myślenie o ryzyku i bardzo dobrym pomysłem jest włączenie swoich wniosków do polityki bezpieczeństwa. To, jak daleko chcesz się posunąć, zależy oczywiście od Ciebie. Firmy muszą obliczyć ryzyko związane z ich obszarem działalności, ale jeśli uważają, że praca, którą wykonują, może być celem tego rodzaju ataku, powinny podjąć środki ostrożności. Jak już wspomniano w tej książce, ochrona przed fizycznym atakiem jest znacznie trudniejsza niż ochrona przed hakerami komputerowymi, ale poniższe oświadczenia dotyczące zasad bezpieczeństwa powinny przynajmniej dać do myślenia:

• Wszystkie opakowania z nieznanego źródła należy przed otwarciem poddać skanowaniu fluoroskopowemu.

• Jeśli podejrzewa się urządzenie - czy to z powodu skanowania fluoroskopowego, czy w inny sposób - należy natychmiast powiadomić ochronę i ewakuować budynek. Dział bezpieczeństwa jest odpowiedzialny za powiadamianie organów ścigania i ratowników.

• Torby lub paczki pozostawione bez nadzoru należy traktować jako potencjalnie niebezpieczne. Cały personel i goście powinni zawsze mieć przy sobie swoje rzeczy. Jeśli podejrzewa się urządzenie - a personel jest zachęcany do zachowania ostrożności - należy natychmiast poinformować ochronę i postępować zgodnie z jego instrukcjami.

• Paczki podejrzane należy pozostawić na miejscu przed ewakuacją. Unikaj niepotrzebnego obchodzenia się i nie potrząsaj ani nie wąchaj opakowania. Po ewakuacji dokładnie umyj ręce.

• Podejrzaną pocztę należy natychmiast zgłosić do działu bezpieczeństwa. Poczta może zostać uznana za podejrzaną, jeśli spełnia którykolwiek z warunków następujące kryteria:

• Nie ma adresu zwrotnego, ograniczających oznaczeń (takich jak „osobisty” lub „poufny”).

• Pochodzi z kraju, z którego firma rzadko otrzymuje pocztę.

• Ma nadmierną opłatę pocztową.

• Jest wysyłany na stanowisko, zwłaszcza jeśli tytuł jest nieprawidłowy.

• Ma słabą pisownię lub pisownię.

• Posiada wystające druty.

• Ma dziwny zapach.

• Na opakowaniu znajduje się tłusta lub krystaliczna pozostałość.

• Jest zabezpieczony nadmiernym sznurkiem lub taśmą.

Oznaczony ochronnie lub sklasyfikowany materiał GDI

Na arenie rządowej, obronnej i wywiadowczej (GDI) praktyka przypisywania różnych poziomów klauzuli bezpieczeństwa informacjom (czy to pisemnym notatkom, drukowanym raportom, czy też danym przechowywanym w systemach informatycznych) jest bardzo dobrze znana. Poziomy klasyfikacji określają sposób udostępniania, przechowywania i uzyskiwania dostępu do informacji. Na arenie GDI powszechną praktyką jest ograniczanie dostępu do takich materiałów na podstawie poziomu poświadczenia bezpieczeństwa osobowego. Specyfikę poświadczeń bezpieczeństwa omówiono w załącznikach, jednak jednym wspólnym wątkiem jest to, że niezależnie od charakteru i wrażliwości informacji, powinny one być udostępniane tylko tym, którzy muszą wiedzieć. Pojęcie „potrzeby wiedzieć” jest bardziej krytyczne dla ochrony informacji niż cokolwiek innego. W sektorze publicznym Zjednoczonego Królestwa materiał objęty oficjalną klasyfikacją określa się jako „znak ochronny”; w Stanach Zjednoczonych nazywa się go po prostu „niejawnym”. Oba rządy, mimo że ich procedury poświadczania bezpieczeństwa są bardzo różne, stosują zasadniczo te same kategorie klasyfikacji danych. Zostały one omówione w kolejnych sekcjach, od klasyfikacji niskiej do wysokiej.

Niesklasyfikowane lub nieoznaczone

Nie jest to klasyfikacja sama w sobie, ale formalne oświadczenie, że treść może być przeglądana przez personel bez poświadczenia bezpieczeństwa osobowego, pod warunkiem oczywiście, że mają niezbędną wiedzę. Czasami dokumenty opatrzone oznaczeniem Niesklasyfikowane mogą być dostępne dla ogółu społeczeństwa. Jednym z przykładów są notatki z kursu CESG CHECK Assault.

Zastrzeżone

To jest pierwszy poziom klasyfikacji. Jest szeroko stosowany w Wielkiej Brytanii w przypadku dokumentów i notatek międzyresortowych, które nie zawierają niczego szczególnie wrażliwego, ale których autor może nie chcieć publicznie udostępniać (lub które mogą być kłopotliwe). Chociaż teoretycznie do przeglądania dokumentów oznaczonych jako Zastrzeżone wymagane jest poświadczenie ekologiczne niskiego poziomu, powszechną praktyką jest udostępnianie ich przez kontrolerów bezpieczeństwa każdemu w wydziale, który potrzebuje znać ich treść. Na przykład notatka wysłana do firm z List-X przez służby wywiadowcze o możliwej wzmożonej działalności terrorystycznej byłaby oznaczona jako Zastrzeżona. W Stanach Zjednoczonych ten poziom klasyfikacji nie był stosowany w kraju od czasów II wojny światowej (chociaż jest używany przez NATO w taki sam sposób, jak rząd Wielkiej Brytanii). Aby zmylić sprawy, rząd Stanów Zjednoczonych używa „Zastrzeżony" jako termin ogólny, obejmujący tajne lub niejawne materiały w ogólności lub w odniesieniu do technologii lub wiedzy, która jest „ograniczona" ze swej natury (na przykład tajemnice jądrowe).

Poufne

Następny poziom klasyfikacji to Poufne (w Stanach Zjednoczonych określany również jako klasyfikacja poziomu 1). Są to informacje, które w przypadku ujawnienia byłyby „szkodliwe" lub „szkodliwe". Ponieważ różne departamenty na różne sposoby wykorzystują klasyfikacje, może być trudno ocenić, co dokładnie oznacza „niszczący". Jednak w praktyce w Wielkiej Brytanii poufne są używane głównie przez organy ścigania, a nie przez wywiad. Jest to informacja, która jest zbyt wysoka, aby można ją było rozpowszechniać ogólnie, a zbyt niska, aby zapewnić bezpieczeństwo narodowe. Następujące informacje zostaną oznaczone jako poufne:

• dane wywiadowcze oddziału specjalnego (znane jako pakiety docelowe) dotyczące brutalnych obrońców praw zwierząt;

• Dane przechowywane w krajowej bazie danych DNA;

• Niektóre rządowe sieci komputerowe w całości.

Sekret

W klasyfikacji Secret (lub Level 2) sprawy stają się trochę bardziej interesujące. Są to informacje, których ujawnienie spowodowałoby „poważne szkody" dla bezpieczeństwa narodowego. Wszystko, co jest oznaczone jako tajne lub powyżej, jest „ograniczoną dystrybucją" (znane również jako kontrolowane przez wytwórcę - ORCON - w Stanach Zjednoczonych). Wszystkie kopie tajnego dokumentu są ponumerowane i przechowywane są zapisy, kto uzyskał dostęp. Ogromna większość materiałów związanych z obronnością jest klasyfikowana jako tajne, podobnie jak rzeczy, które rząd Wielkiej Brytanii naprawdę chciałby ukryć przed swoimi obywatelami. Przykłady obejmują:

• Wyniki i dane dotyczące bezpieczeństwa projektu Euro Fighter;

• Specyfikacje techniczne dotyczące krajowych dowodów osobistych (pozostawionych następnie w pociągu i znalezionych przez dziennikarza);

• Budżetowanie wojskowe.

Ściśle tajne

Pomimo tajemniczości otaczającej słowa Top Secret, bardzo niewiele jest faktycznie sklasyfikowane na tym poziomie, przynajmniej w porównaniu do Secret. Sama logistyka personelu rozliczeniowego w celu przeglądania materiałów ściśle tajnych jest z wielu powodów przeszkodą. Wiele z tego, co jest

klasyfikowane jako ściśle tajne, wynika nie tyle z treści, ile ze sposobu uzyskania lub z innych całkiem nieoczekiwanych powodów. Na przykład raz widziałem zdjęcia zrobione z samolotu szpiegowskiego, które zawierały tylko jałowe skały oznaczone jako ściśle tajne, ponieważ doświadczony analityk byłby w stanie wydedukować informacje o możliwościach samego samolotu z tych zdjęć. Inne przykłady ściśle tajnej dokumentacji obejmują:

• Krótkoterminowe taktyczne dane wojskowe;

• Eksperymenty naukowe, które mogą wywołać oburzenie społeczne, na przykład wykorzystanie kóz w komorach dekompresyjnych w celu stworzenia scenariuszy przetrwania dla nurków wojskowych;

• Możliwości łamania kodu.

Top Secret to najwyższe oficjalne oznaczenie ochronne większości produktów zachodnich krajów. Jednak Top Secret sam w sobie jest wielopoziomowy (w Wielkiej Brytanii nazywane są one poziomami STRAP), a niektóre projekty w przeszłości były realizowane znacznie powyżej tego poziomu, czego przykładem jest próba złamania kodu w Bletchley Park podczas II wojny światowej, gdzie Brytyjscy naukowcy złamali niemieckie kody Enigmy. Ten projekt jest teraz określany jako Ultra Secret.

Rozliczenie słów kodowych

Dane oznaczone ochronnie mogą być dalej dzielone poprzez użycie słów kodu. To dodatkowo ogranicza dystrybucję dokumentacji. Słowa kodowe są używane zarówno w Wielkiej Brytanii, jak i w Stanach Zjednoczonych (choć w Stanach Zjednoczonych jest ich znacznie więcej). Mogą odnosić się do konkretnego projektu, który wymaga od członków przejścia oddzielnej procedury zatwierdzania lub do określonych technologii objętych ograniczeniami, lub mogą być zastrzeżeniami narodowościowymi, które ograniczają informacje ze względu na kraj pochodzenia. Przykłady obejmują:

• ONLY UK EYES - tylko do rozprowadzania wśród osób narodowości brytyjskiej;

• NATO SECRET - dostępne tylko dla tych w krajach NATO lokalnie zatwierdzonych jako tajne i wyżej;

• LOCSEN - Lokalna wrażliwość, tj. Nie do ujawnienia lokalnym urzędnikom;

• ATOMAL - informacje o technologii broni jądrowej;

• DEDIP - tylko do pokazania wyznaczonym urzędnikom;

• NOFORN - brak cudzoziemców (zabawnie zinterpretowany jako „No Fornication" Cliffa Stolla w jego książce The Cuckoo's Egg z 1989 roku);

• LES - wrażliwy na egzekwowanie prawa.

Oznaczenia ochronne w świecie korporacji

Informacje w poprzedniej sekcji są krytyczne dla każdego, kto wykonuje prace związane z zabezpieczeniami dla GDI. Jednak wiele organizacji handlowych również wdraża system oznaczeń ochronnych, choć znacznie mniej skomplikowanych i oficjalnych, do czego gorąco zachęcam. Idealnym miejscem do kodyfikacji tego systemu jest oczywiście polityka bezpieczeństwa. Poniższe przykłady komercyjnych klasyfikacji są powszechne, choć oczywiście różnią się one znacznie w zależności od potrzeb różnych organizacji. Oznaczenia ochronne należy wyraźnie dodać na górze i na dole dokumentów oraz na stronie tytułowej lub stronie tytułowej faksu. Oznaczenia ochronne wiadomości e-mail są nieco bardziej złożone, ponieważ wrażliwe wiadomości e-mail są najprawdopodobniej zaszyfrowane. W każdym przypadku należy unikać wysyłania wrażliwych danych pocztą elektroniczną, chyba że w zaszyfrowanym załączniku, w którym przypadku zastosowanie mają powyższe zasady.

Firma poufna

E-maile i dokumenty najprawdopodobniej będą zawierać to oznaczenie. Firma poufna oznacza, że treść odnosi się do działalności firmy i że rozpowszechnianie jest ograniczone do pracowników firmy. To oznaczenie powinno być używane do ogłoszeń, dyskusji i podręczników dotyczących całej firmy, dotyczących procedur operacyjnych i praktyk biznesowych oraz wszystkiego, co nie jest szczególnie wrażliwe na projekt. Wyciek informacji poufnych firmy powinien być sprawą dyscyplinarną; jednak duże firmy powinny mieć świadomość, że w żaden sposób nie zapobiegnie to wyciekom.

Ograniczona dystrybucja

Projekty wrażliwe wewnętrznie należy oznaczyć jako „tylko oczy odbiorcy". Każda kopia powinna być ponumerowana, a lista dystrybucyjna powinna być ściśle kontrolowana. Takie dokumenty mogą zawierać tajemnice handlowe lub dane handlowe, których utrata byłaby finansowa dla firmy. Inne dokumenty, które potencjalnie mogą być oznaczone jako Recipient Eyes Only, obejmują plany strategiczne na poziomie korporacyjnym, notatki, dane finansowe i informacje o zakupach.

Handlowych w tajemnicy

To oznaczenie jest zwykle używane, gdy firmy przekazują sobie nawzajem poufne informacje. Najczęstszym przykładem są usługi doradcze dotyczące pracy zleconej osobie trzeciej. Firmy powinny wymagać od wszystkich stron trzecich, które angażują się w usługi doradcze, do podpisania umowy o nieujawnianiu, której klauzula stanowi, że cała komunikacja będzie oznaczona jako poufna.

Restricted Pre Embargo

To oznaczenie jest w zasadzie takie samo, jak „Tylko oczy odbiorcy", z wyjątkiem tego, że dane są klasyfikowane na określony czas. Jest to powszechne w firmach, które chcą zachować informacje o produktach z dala od mediów aż do oficjalnej daty premiery.

Polityka znakowania firmy

W zasadach bezpieczeństwa można zawrzeć następujące zasady:

• Oznaczenia ochronne są przypisywane przede wszystkim na podstawie poziomu wrażliwości danych, ale mogą być również określane przez obszar biznesowy i zobowiązania umowne. Ważne jest, aby upewnić się, że poziom klauzuli przypisany poszczególnym informacjom jest odpowiedni. Należy wziąć pod uwagę konieczność przeklasyfikowania informacji w całym cyklu ich życia.

• Wszystkie poufne dokumenty powinny być wyraźnie oznaczone jako takie na okładce i na każdej stronie, zarówno powyżej, jak i poniżej tekstu.

• Dokumenty poufne należy przechowywać w bezpiecznym miejscu, gdy nie są używane i nigdy nie należy ich pozostawiać na biurku. Dokumenty oznaczone jako poufne dla firmy oraz „Confidence" należy przechowywać w zamkniętej szufladzie lub szafce. Przechowywanie dokumentacji specyficznej dla projektu leży w gestii lidera projektu.

• Wszelkie kopie dokumentów oznaczonych ochronnie lub pochodzące z takich dokumentów muszą posiadać to samo oznaczenie ochronne. Żadne kopie materiałów o ograniczonej dystrybucji nie mogą być wykonywane bez zgody autora.

• Chronione informacje przechowywane w formacie elektronicznym powinny być drukowane tylko wtedy, gdy jest to konieczne, aby zminimalizować liczbę istniejących kopii.

Tematy poruszone tutaj poszerzam w następnej sekcji, w której omawiam różne elementy bezpieczeństwa komunikacji. Złożoność i wymagania systemu znakowania ochronnego powinny stać się jasne.

Bezpieczeństwo komunikacji

Komunikacja odnosi się do mnogości technologii używanych na co dzień w biznesie. Każda forma technologii komunikacyjnej ma potencjał do nadużycia jako kanał ataku. Ważne jest, aby autorzy polityki bezpieczeństwa rozumieli te zagrożenia i dokumentowali je w polityce bezpieczeństwa. Problemy mogą wynikać z natury samej technologii lub mogą wynikać z niewłaściwych praktyk bezpieczeństwa. W każdym razie edukacja użytkownika i egzekwowanie zasad znacznie zmniejszy ryzyko narażenia. Technologia komunikacyjna przeszła bardzo długą drogę w ciągu ostatnich 10 lat, a przy wszechobecnym charakterze Internetu sam termin może odnosić się do rzeczy, których autor polityki bezpieczeństwa mógł nawet nie wziąć pod uwagę.

Zabezpieczanie korzystania z telefonu

Celem polityki bezpieczeństwa telefonu jest zapewnienie, że personel:

• Weryfikacje tożsamości osób dzwoniących i tych, do których dzwonią;

• Wie, o czym można, a czego nie można rozmawiać przez telefon;

• Podejmuje kroki w celu ochrony informacji wymienianych przez telefon we właściwy sposób.

Wiele z tego jest oczywistych, ale niektóre są bardziej subtelne. Niemniej jednak najlepsza praktyka nakazuje dokumentowanie i przestrzeganie polityki bezpieczeństwa telefonu. Podczas gdy ochrona przed atakami socjotechnicznymi jest oczywistym problemem, nie jest to jedyny problem, jeśli wziąć pod uwagę takie rzeczy, jak poczta głosowa. Kiedy wprowadzasz Voice-over-IP (VoIP), granice między technologiami, a nawet bariery organizacyjne, stają się jeszcze bardziej zatarte. Poniższe oświadczenia dotyczą polityki bezpieczeństwa telefonu:

• Nie należy używać głośników podczas omawiania wrażliwych tematów lub projektów.

• Personel powinien unikać omawiania poufnych informacji w zasięgu słuchu osób, które nie zostały wyraźnie określone dla danego projektu.

• Korzystanie z publicznych usług VoIP (o ile nie zostało to specjalnie zatwierdzone) jest zabronione w interesach firmy.

• Hasła i inne informacje o uprzywilejowanym dostępie nigdy nie powinny być przekazywane przez telefon. Wszelkie takie wnioski należy niezwłocznie zgłaszać swojemu przełożonemu.

• Osobom dzwoniącym nie należy nigdy udostępniać poufnych informacji firmowych, takich jak listy telefonów, numery wewnętrzne lub informacje o personelu. Przekaż wszystkie takie prośby do recepcji.

• Skrzynki poczty głosowej powinny być zabezpieczone kodem dostępu znanym tylko użytkownikowi i regularnie zmienianym.

• Wrażliwe informacje nie powinny być nigdy pozostawiane jako wiadomość głosowa, niezależnie od odbiorcy.

Zabezpieczanie korzystania z poczty elektronicznej

W wielu organizacjach poczta elektroniczna jest numerem jeden dla wirusów, koni trojańskich i innych zagrożeń dla bezpieczeństwa informacji. Jednak może pojawić się wiele innych problemów: poufne informacje mogą łatwo zostać ujawnione - celowo lub przypadkowo - a poczta e-mail jest potężnym narzędziem inżynierii społecznej, biorąc pod uwagę łatwość, z jaką można podrabiać adresy i podszywać się pod inne osoby. Poniższa lista oświadczeń o ochronie prywatności to absolutne minimum z naciskiem na bezpieczeństwo.

• E-mail nie nadaje się do długoterminowego przechowywania dokumentacji. Nigdy nie należy używać osobistych kont e-mail do przechowywania, przetwarzania ani wysyłania lub otrzymaj firmowy e-mail.

• Biznesowego adresu e-mail nie należy używać do użytku osobistego.

• Wszystkie przychodzące i wychodzące wiadomości e-mail powinny być skanowane pod kątem wirusów i inna złośliwa zawartość. W żadnym wypadku nie należy używać poczty e-mail do wysyłania lub odbierać programy lub inne pliki wykonywalne. W każdym razie takie treści zostaną usunięte przez serwer pocztowy.

• Wysyłając dane pocztą elektroniczną, użytkownicy powinni zachować dyskrecję i poufność równą lub przewyższającą te, które są stosowane do fizycznego dokumenty.

• Informacje uważane za poufne lub wrażliwe muszą być chronione podczas transmisji z wykorzystaniem szyfrowania odpowiedniego do ich oznaczenia ochronnego.

• Adresy e-mail można łatwo podrobić. Przed wysłaniem poufnych informacji upewnij się, że odbiorca jest prawdziwy. Korzystanie z szyfrowania i zaufanych kluczy publicznych jest wymagane w przypadku materiałów oznaczonych w celach ochronnych. Jeśli ktoś zażąda poufnych informacji i twierdzi z jakiegokolwiek powodu, że nie może odebrać zaszyfrowanych plików, należy to natychmiast zgłosić przełożonemu.

• Informacje poufne lub wrażliwe mają być przekazywane tylko tym osobom, które mają uzasadnioną potrzebę ich poznania. Należy unikać list dystrybucyjnych, które nie zapewniają prywatności list odbiorców.

Kompletna polityka e-mailowa powinna również zawierać klauzule dotyczące zniesławienia i prawne, które nie są dla nas szczególnie interesujące.

Zabezpieczanie faksów

Bezpieczeństwo faksu jest często pomijane na poziomie operacyjnym i politycznym. Nie jest to całkowicie zaskakujące, biorąc pod uwagę, jak mało jest obecnie używanych faksów w porównaniu z pocztą elektroniczną. Jednak nadal każdy musi mieć możliwość wysyłania i odbierania faksów, a ich używanie może powodować problemy z bezpieczeństwem:

• Faksy nie są bezpieczne (tj. zaszyfrowane) podczas transmisji.

• Faksy nie są bezpieczne przy odbiorze - często faks znajduje się w obszarze publicznym, z którego każdy może uzyskać do niego dostęp. Jak zwykle, odrobina świadomości może pomóc, podobnie jak następujące oświadczenia polityczne:

• Faksy powinny znajdować się w bezpiecznych miejscach, do których mają dostęp tylko upoważnieni pracownicy.

• Personel powinien zweryfikować numer faksu odbiorcy przed wysłaniem.

• Odbiorca dokumentu zawierającego chronione informacje (np. Tylko dla oczu odbiorcy) musi zostać powiadomiony telefonicznie przed wysłaniem dokumentu.

• Jeśli to możliwe, faksy nigdy nie powinny być przekazywane w imieniu osoby trzeciej. Jeśli jednak jest to wymagane, należy uzyskać odpowiedni dowód tożsamości od żądającego.

• Hasła i inne informacje o uprzywilejowanym dostępie nigdy nie powinny być przesyłane faksem.

Zabezpieczanie wiadomości błyskawicznych

Oprogramowanie do obsługi wiadomości błyskawicznych to kolejny obszar, w którym w ostatnich latach nastąpił ogromny wzrost, do tego stopnia, że każdy korzysta z co najmniej jednego komunikatora na swoim komputerze, zarówno w biurze, jak i poza nim. Niektóre firmy posunęły się tak daleko, że przyjęły określoną technologię komunikatorów internetowych jako oficjalny lub półoficjalny sposób szybkiej wymiany informacji (a menedżerowie lubią mieć możliwość przeglądania listy nazwisk i sprawdzania, kto siedzi przy ich biurkach). Nie ma w tym nic złego, o ile rozumiane jest ryzyko, co niestety rzadko się zdarza. Na przykład widziałem kilka firm używających komunikatora MSN Live Messenger jako klienta komunikatora internetowego, nie zdając sobie sprawy, że przekazuje on wiadomości przez Internet w postaci niezaszyfrowanej, nawet jeśli nadawca i odbiorca siedzą obok siebie w tej samej sieci za zaporą. Innym problemem jest to, że jeśli osoba atakująca jest w stanie uzyskać hasło do konta komunikatora internetowego użytkownika (co w przypadku usługi MSN może być tak proste, jak włamanie się do konta hotmail), ma natychmiastowy dostęp do wszystkich ich kontaktówy; inżynier społeczny mógłby to wykorzystać, aby uzyskać uprzywilejowane informacje. Po zapukaniu MSN czuję się zobowiązany do zaoferowania rozwiązania, jeśli go używasz. Oprogramowanie SimpLite jest dostępne bezpłatnie do użytku domowego lub komercyjnego i dodaje szyfrowanie typu end-to-end dla kilku klientów komunikatorów (w tym MSN Live Messenger). Możesz go pobrać ze strony www.secway.fr. Jakkolwiek komunikatory są używane w Twojej organizacji, warto wspomnieć o tym w polityce bezpieczeństwa, choćby po to, by powtórzyć to, co powiedzieliśmy o poprzednich technologiach:

• Hasła i inne informacje o uprzywilejowanym dostępie nigdy nie powinny być przesyłane za pośrednictwem komunikatorów internetowych.

• Użytkownicy powinni zweryfikować tożsamość wszystkich użytkowników, których dodają do swoich list kontaktów.

• Nagłe lub nieodpowiednie prośby o informacje uprzywilejowane należy natychmiast kierować do swojego bezpośredniego przełożonego.

• Żadne załączniki nie powinny być wysyłane ani odbierane za pośrednictwem wiadomości błyskawicznych.

• Nie zezwalaj programowi do obsługi wiadomości błyskawicznych na zapamiętywanie hasła lub automatyczne logowanie się do konta.

• Nie akceptuj automatycznie wiadomości przychodzących od nazw logowania, których nie ma na Twojej liście kontaktów. Jeśli ktoś chce zacząć komunikować się z Tobą za pośrednictwem komunikatorów, powinien wysłać do Ciebie wiadomość e-mail lub telefon w celu wymiany nazw logowania.

• Nie klikaj linków wysłanych do Ciebie w wiadomości, nawet jeśli wydają się pochodzić od kogoś, kogo znasz.

Weryfikacja pracowników

Polityka bezpieczeństwa personelu obejmuje szereg kwestii, które odnoszą się bezpośrednio do pracowników oraz ich obowiązków i obowiązków w firmie w zakresie ochrony informacji i promowania bezpieczeństwa informacji w ogóle. Całkiem dużo z tego zostało już omówione w tym rozdziale. W tej części omówiono proces rekrutacji, w którym po raz pierwszy stosuje się praktykę bezpieczeństwa personelu. Weryfikacja przeszłości stała się absolutnie krytyczna w procesie rekrutacji, a nie tylko w obszarach, w których kandydat będzie miał dostęp do poufnych informacji. Istnieje kilka powodów, dla których przeprowadza się weryfikację przeszłości:

• Potwierdzenie informacji podanych w trakcie rekrutacji. Co najmniej powinno to potwierdzać tożsamość kandydata, posiadane kwalifikacje i historię zatrudnienia.

• Należyta staranność w celu zapobieżenia procesom sądowym, które mogą powstać w wyniku zatrudniania osób, które przedstawiały się fałszywie.

Poza stanowiskami w sektorze publicznym, gdzie formalne poświadczenie bezpieczeństwa można zastosować procedury (patrz załączniki), sprawdzenie przeszłości jest przeprowadzane przez własny dział zasobów ludzkich organizacji lub (co jest bardziej prawdopodobne) zlecane firmie specjalizującej się w tego rodzaju pracy. Sprawdzanie przeszłości musi być opłacalne i przeprowadzane szybko, więc oczywiście jest wiele rzeczy, których po prostu nie będzie można się dowiedzieć. Należy jednak zweryfikować przynajmniej następujące informacje:

• Historia zatrudnienia - Zwróć szczególną uwagę na luki w zatrudnieniu. Nie wystarczy, że daty się pokrywają. Upewnij się, że tytuły stanowisk podane na liście kandydatów są dokładne.

• Certyfikacja zawodowa - Sprawdź ważność i status.

• Kwalifikacje akademickie - Sprawdź ważność kwalifikacji na poziomie wyższym lub wyższym. Wszystko poniżej poziomu studiów nie jest tak naprawdę ważne, ale zawsze weryfikuj uczelnie, daty, tytuły i stopnie. Nie wierz po prostu w żadne transkrypcje ani imponujące dokumenty, które otrzymałeś. Można je złożyć w około 10 minut. Transkrypcje studentów są dostępne w biurach uniwersytetu. Niektóre firmy rygorystycznie podchodzą do uzyskiwania referencji, ale poza walidacją zatrudnienia nie są one zbyt wiele warte z mojego doświadczenia i nie należy ich przykładać zbytniej wagi. Jeśli jest wystarczająco dużo czasu (i wymagań), organizacja może również chcić zażądać informacji na temat:

• Historia kredytowa - osoba z historią problemów z zarządzaniem długiem może być z natury niewiarygodna lub podatna na zewnętrzne zachęty finansowe.

• Rejestr karny - z oczywistych powodów.

Przepisy różnią się w zakresie informacji, jakich pracodawca może zażądać od potencjalnego pracownika. Na przykład w Wielkiej Brytanii (większość) wyroków skazujących może zostać wstrzymana od pracodawcy po określonym czasie; w Holandii państwo może zapewnić kontrolę przeszłości, która jest specjalnie dostosowana do stanowiska. Idealnie byłoby, gdyby wszyscy nowi pracownicy podlegali jakiejś formie kontroli przeszłości, chociaż nie zawsze jest to możliwe. Sprawdzanie przeszłości z pewnością powinno być wykonywane w następujących okolicznościach:

• Organizacja zajmuje się doradztwem i ma do czynienia z poufnymi danymi klientów.

• Pracownik miałby dostęp do poufnych danych.

• Pracownik miałby dostęp do danych finansowych lub płacowych.

Pamiętaj, że jest o wiele prostsze i lepsze dla wszystkich, jeśli pracodawcy wiedzą, kogo zatrudniają (lub odrzucają) z góry, a nie sześć miesięcy lub rok później, nawet jeśli zajmuje to trochę czasu i jest niewygodne.

Niszczenie danych

Jeśli organizacje sformalizowały (i przestrzegały) działań określonych w tym dokumencie sekcja uczyniłaby życie przestępcami i inżynierami społecznymi (i testerzy penetracji) dużo trudniej. Niestety, większość tego nie robi. Prowadzi to do tego, że poufne dane na papierze, nośnikach cyfrowych lub dyskach twardych regularnie wpadają w niepowołane ręce. Przedstawię solidne wytyczne dla każdego rodzaju mediów.

Usuwanie danych na nośnikach cyfrowych

Zbyt wiele firm wyrzuca dyski twarde do śmieci, gdy dobiegają końca lub w szafce nie ma miejsca na stary sprzęt, którego nikt nie będzie używał ponownie. Bardzo niewielu zadaje sobie trud, aby najpierw usunąć zawartość, chociaż kilka może wykonać pobieżny format (który usuwa niewiele). Są też firmy, które sprzedają swoje stare nośniki danych w serwisie eBay. To nie jest najmądrzejszy pomysł. Jeśli naprawdę musisz sprzedawać stary sprzęt, upewnij się, że dyski są czyszczone kryptograficznie za pomocą narzędzia takiego jak DBAN. Poniższe zasady mogą pomóc w ochronie odrzuconych danych:

• Dyskietki, napędy USB i taśmy magnetyczne należy oczyścić kryptograficznie przed ponownym użyciem za pomocą [włóż preferowane narzędzie]. W przypadku uszkodzeń fizycznych dyski należy zniszczyć przez spalenie.

• Płyty CD i DVD należy rozdrobnić lub pociąć na ćwiartki przed utylizacją.

• Dyski twarde należy wyczyścić kryptograficznie przed ponownym użyciem

[włóż preferowane narzędzie]. Jeśli są fizycznie uszkodzone, te dyski powinny być zniszczone przez spalenie.

Utylizacja danych na papierze

Bezpieczne obchodzenie się z odpadami papierowymi ma kluczowe znaczenie, zwłaszcza że zużywa się go o wiele więcej niż nośniki cyfrowe. Odręczne notatki, które mogą zawierać wszystko, od numerów telefonów i haseł po poufne projekty raportów, muszą być bezpiecznie usuwane. Jedną z rzeczy, do których najbardziej bym zachęcał, jest ograniczenie zużycia papieru tam, gdzie to możliwe. Jednak biuro bez papieru to mrzonka i dlatego pozbycie się poufnych informacji jest naprawdę problemem każdego. Rozważ następujące oświadczenia dotyczące zasad bezpieczeństwa

• Papieru nie wolno wkładać do zwykłych pojemników na makulaturę, ponieważ istnieje możliwość, że informacje mogą zidentyfikować osobę lub zawierać dane biznesowe.

• Jeśli informacje zostaną uznane za poufne, konieczne jest zniszczenie ich na bardzo małe kawałki przed umieszczeniem w odpowiednim pojemniku na odpady poufne.

• Tylko niszczarki krzyżowe dostarczone przez [wstaw preferowanego dostawcę] są dostępne aby służyć do bezpiecznego niszczenia papieru. Nieautoryzowane niszczenie sprzętu zapewnia niewystarczający stopień zabezpieczenia zgodnie z tą polityką.

Szyfrowanie danych

W przypadku zgubienia lub kradzieży laptopa lub dysku USB pierwsze zgłaszane obawy dotyczą raczej zawartych w nim danych, a nie strat finansowych spowodowanych przez sam sprzęt. Przynajmniej

mam taką nadzieję. Istnieje szereg rozwiązań technicznych gwarantujących, że nawet w przypadku kradzieży laptopa lub innego nośnika niemożliwe jest odzyskanie jego zawartości. Takie rozwiązania obejmują zarówno zabezpieczenie plików, katalogów i partycji, jak i szyfrowanie całego dysku twardego i zdecydowanie polecam to drugie. Obecnie popularnym „rozwiązaniem" jest użycie haseł ATA, które blokują talerze samego dysku twardego, aby uniemożliwić dostęp do danych. Jednak jest to trywialne do ominięcia, a same dane bazowe nie są szyfrowane. Nigdy nie należy na nim polegać. Wdrożenie szyfrowania dysków twardych w całym przedsiębiorstwie znacznie zwiększy spokój ducha, jeśli chodzi o bezpieczeństwo danych, ale z pewnością zwiększy obciążenie pracą związaną z obsługą użytkowników. Dlatego ważne jest, aby użytkownicy przeszli szkolenie w tej technologii, a jej implementacja została sformalizowana w polityce bezpieczeństwa. Sugerowane są następujące zasady:

• Wszystkie urządzenia użytkownika są dostarczane z zainstalowanym szyfrowaniem dysku twardego [wstaw preferowane narzędzie]. Użytkownicy nie powinni próbować modyfikować ani manipulować tą instalacją, ale są zobowiązani do korzystania z niej w dostarczony sposób.

• Hasła i tokeny wymagane do uzyskania dostępu do zaszyfrowanych mediów powinny być utrzymywane w tajemnicy i nie powinny być udostępniane innym osobom, w tym innym użytkownikom.

• Dodatkowe woluminy niezwiązane z siecią (takie jak urządzenia pamięci masowej USB) powinny być zintegrowane z [wstaw preferowane narzędzie] i zaszyfrowane. Poziom zastosowanego szyfrowania może zależeć od wrażliwości danych, jednak użytkownicy powinni zawsze popełniać błędy po stronie wyższego poziomu szyfrowania, niż może to być konieczne.

Ryzyko związane z outsourcingiem

Jednym z powszechnych obszarów słabych punktów (pod wieloma względami najtrudniejszym do rozwiązania) jest kwestia zarządzania ryzykiem w przypadku zatrudniania wykonawców i firm zewnętrznych do pracy z systemami informatycznymi. Outsourcing kiedyś był wyłącznie świadczeniem usług dla dużych firm, ale obecnie organizacje z całego spektrum świata biznesu zlecają przynajmniej niektóre funkcje zewnętrznemu dostawcy i wiąże się to z różnymi ryzykami. Nie chodzi tylko o to, czy wykonawca jest godny zaufania - większość z nich jest. Zatrudniając kosztowny zasób tymczasowy (często do pilnej pracy), często jest znacznie mniej czasu, aby upewnić się, że znają i przestrzegają zasad bezpieczeństwa oraz traktują dane z taką samą ostrożnością, jakiej można oczekiwać od pracowników pełnoetatowych. Inną obawą jest to, że chociaż można ogólnie określić, co można, a czego nie można wnieść do firmy, to jest to znacznie trudniejsze do wyegzekwowania w przypadku wykonawców, których specjalistyczny sprzęt może być wymagany do wykonania zadania. Z drugiej strony, zatrudniając usługodawcę do jakiegokolwiek zadania, które wiąże się z przetwarzaniem danych (które mogą być poufne), niezwykle ważne jest uzyskanie pewności, że ich własne obiekty i systemy informatyczne posiadają mechanizmy kontrolne zapewniające bezpieczeństwo. Kuszące jest myślenie, że ten problem dotyczy tylko strony trzeciej dostawców usług komputerowych i oprogramowania, ale to nie może być dalsze od prawdy. Każda funkcja, którą zlecasz na zewnątrz, potencjalnie stawia dane Twoje (lub klienta) w nieznane ręce. Wydaje się, że wiele firm nie ma problemu z indyjskimi centrami telefonicznymi wypełnionymi nisko opłacanymi pracownikami przyjmującymi zamówienia na karty kredytowe od klientów lub przetwarzającymi inne poufne dane. Doprowadziło to do strasznych naruszeń bezpieczeństwa i wielu przypadków kradzieży tożsamości. Inny, nieco mniej istotny, ale bardzo zabawny (i dobrze udokumentowany) incydent miał miejsce, gdy wydawca gier komputerowych zlecił produkcję dzieł sztuki firmie deweloperskiej w Azji Południowo-Wschodniej. Dopiero po opublikowaniu gry stało się jasne, że praktycznie cała zawartość artystyczna została

skradziona z innych znanych gier i filmów. Dostajesz to, za co płacisz, a to ryzyko, które podejmujesz, oddając dobro swojej firmy w ręce osób, których nie znasz. Poniższe zasady zawierają pewne wskazówki dotyczące ochrony w przypadku korzystania z outsourcingu stron trzecich:

• Wszystkie strony trzecie są zobowiązane do przestrzegania firmowych polityk bezpieczeństwa, zasad, przepisów i procedur kontroli zmian. Firma zapewni niezbędne narzędzia, aby pomóc w zapewnieniu zgodności w stosownych przypadkach.

• Osoby trzecie są zobowiązane do podjęcia wszelkich niezbędnych kroków w celu zapewnienia bezpieczeństwa powierzonych im danych firmowych. Wszystkie dane będą traktowane w sposób zgodny z ich oznaczeniem ochronnym. Firma zapewni podmiotom trzecim niezbędne narzędzia, gdzie istotnych.

• Osoby trzecie muszą dostarczyć firmie listę wszystkich pracowników zatrudnionych przy umowie. Ta lista musi być natychmiast aktualizowana w przypadku wszelkich zmian.

• Wszyscy pracownicy zewnętrzni pracujący nad projektami firmy mogą podlegać kontroli przeszłości lub formalnym poświadczeniom bezpieczeństwa. Brak uzyskania (lub przedłożyć wymaganą dokumentację dotyczącą) pozytywnego sprawdzenia przeszłości lub poświadczenia bezpieczeństwa, które uniemożliwi pracownikowi pracę nad projektami firmy.

• Wszyscy pracownicy będący osobami trzecimi zwrócą lub zniszczą (w stosownych przypadkach) całą posiadaną dokumentację na żądanie lub w momencie opuszczenia dostawcy.

• Wszystkie prace osób trzecich powinny być jednoznacznie identyfikowalne dla poszczególnych pracowników członków. Będzie to egzekwowane zarówno proceduralnie, jak i poprzez dostęp i kontrolę.

Zasady reagowania na incydenty

Zasady reagowania na incydenty określają kroki, które należy wykonać w przypadku podejrzenia incydentu związanego z bezpieczeństwem. Incydent może przybierać różne formy, od utraty danych do naruszenia bezpieczeństwa systemu, dlatego ważne jest, aby przeprowadzić analizę ryzyka w celu określenia możliwych zagrożeń i procedur eskalacji, których będziesz przestrzegać w przypadku podejrzenia naruszenia. Zróżnicowany charakter incydentów bezpieczeństwa sprawia, że odpowiedzi są trudniejsze do udokumentowania, ale jest o wiele łatwiej, gdy zrozumiesz, gdzie istnieje potencjalne ryzyko. Następujące zdarzenia można uznać za incydenty naruszające bezpieczeństwo i wyraźnie różne są sposoby ich obsługi:

• Utracone lub skradzione dane - jeśli jakikolwiek sprzęt, nośniki danych lub dokumentacja papierowa zawierająca informacje uprzywilejowane, wrażliwe lub poufne zaginie, należy to uznać za incydent związany z bezpieczeństwem (w rzeczywistości jest to najbardziej powszechna forma). Do czynników łagodzących, które zmniejszyłyby wagę lub poziom ryzyka, należałyby szyfrowanie. Jeśli złodziej lub szpieg korporacyjny ma laptop pełen tajemnic firmy, ale nie ma możliwości ich odzyskania, jest to zdecydowanie mniejsze ryzyko. To jedna z zalet uwierzytelniania opartego na tokenach. Gdy laptop zostanie wykryty jako zgubiony lub skradziony, token może zostać zniszczony, aby upewnić się, że nie ma dalszej możliwości uzyskania dostępu do danych.

• Próba włamania do sieci - niemal ciągły atak z Internetu to fakt. Typy ataków są różne, ale najprawdopodobniej będą to inne zainfekowane komputery poszukujące nowych hostów do ataku. Dobre zasady bezpieczeństwa granic i poprawek negują ogromną większość tego ruchu i niewiele można zyskać na eskalowaniu każdego skanowania portu lub próby przepełnienia bufora, które widzisz

(jeśli wdrażasz technologię wykrywania włamań, należy przechowywać rejestr wszystkich ataków). Jeśli zauważysz powtarzające się ataki z tych samych zakresów sieci (a przyzwoite systemy wykrywania włamań (IDS) powiedzą Ci, czy tak się dzieje), powinieneś rozważyć podjęcie działań łagodzących, takich jak zablokowanie zasięgu na zaporze lub powiadomienie odpowiedniego dostawcy usług internetowych .

• Podejrzewane lub potwierdzone włamanie - jeśli uważasz, że komputer lub inne urządzenie w Twojej organizacji zostało naruszone, należy je natychmiast usunąć z sieci i zastosować odpowiednie procedury kryminalistyczne. Często jest to poza możliwościami działów IT i należy zasięgnąć porady specjalistów. Jednak zainfekowane maszyny powinny, jeśli to możliwe, zostać wycofane i nie podłączać ich ponownie do sieci. Jeśli nie jest to wykonalne finansowo, urządzenie powinno zostać wyczyszczone kryptograficznie i odbudowane z oryginalnego nośnika instalacyjnego. Incydenty, które są najbardziej prawdopodobne w tej kategorii, to wykrycie kluczy rejestrujących lub koni trojańskich, które są zwykle instalowane przez nieświadomy personel - chociaż czasami są wdrażane przez personel ze złośliwych powodów.

• Naruszenie bezpieczeństwa fizycznego - może to być po prostu kradzież lub włamanie, w którym to przypadku powinno być traktowane jak każde inne przestępstwo przeciwko mieniu. Jeśli jednak naruszenie bezpieczeństwa nastąpi na obszarach, na których znajduje się sprzęt komputerowy lub dostęp do sieci, może być konieczne podjęcie dalszych kroków, ponieważ osoby badające naruszenie powinny mieć świadomość, że mogły również wystąpić dodatkowe naruszenia bezpieczeństwa elektronicznego. Jakie kroki firma podąża i reaguje na incydenty bezpieczeństwa, zależy od nich, ale sugeruję, aby upewnili się, że ich planowanie zawiera działania następujące:

• Dokonanie wstępnej oceny w oparciu o podstawowe dowody;

• Zaangażowanie odpowiednich członków zespołu;

• powstrzymanie szkód;

• Ochrona dowodów, w stosownych przypadkach;

• Dążenie do minimalnych zakłóceń w działalności.

Podsumowanie

Przedstawiono koncepcję polityki bezpieczeństwa, co pociąga za sobą jej pisanie i o czym należy pomyśleć. Pisanie polityki bezpieczeństwa może być trudnym zadaniem, a w praktyce są one zwykle rozwijane w miarę upływu czasu, gdy organizacja zaczyna rozumieć zagrożenia, z którymi się boryka, i reagować na nie. Oczywiście nie wszystko dotyczy wszystkich i różne organizacje będą chciały skupić się na różnych aspektach tego rozdziału, zgodnie z ich wymaganiami biznesowymi. To powiedziawszy, dobrze jest przynajmniej poruszyć każdy z omówionych przez nas obszarów. Omówiono następujące tematy:

• Bezpieczeństwo fizyczne - oświadczenia i porady dotyczące zasad dotyczących bezpośrednio CCTV, ochrona obwodowa i ochrona identyfikatorów.

• Materiały niejawne - jak postępować z poufnymi i wrażliwymi informacjami oraz bezpośrednie znaczenie znaków ochronnych w świecie korporacji.

• Bezpieczeństwo komunikacji - Deklaracje polityki w obszarach związanych z komunikacją, w tym telefonami i faksami, ale także komunikatorami, usługami VoIP i innymi technologiami.

• Weryfikacja przeszłości - zalety i wady oraz jakie pytania należy zadawać.

• Bezpieczne niszczenie danych - jak pozbyć się lub bezpiecznie ponownie wykorzystać media elektroniczne.

• Szyfrowanie - kiedy i gdzie szyfrowanie danych powinno być obowiązkowe

• Outsourcing - ryzyko i zapewnienie, że strony trzecie będą przestrzegać Twoich zasad bezpieczeństwa.

• Incydenty bezpieczeństwa - co stanowi zdarzenie naruszające bezpieczeństwo i jak najlepiej na nie reagować.