Kontrwywiad

Omówiliśmy już szereg różnych ataków i sposoby ich wdrażania przeciwko organizacji. Teraz omówionomy kilka sposobów, w jakie organizacje mogą się chronić. Do tej pory z pewnością zdajesz sobie sprawę, że wdrożenie bezpieczeństwa we wszystkich jego formach może stać się monumentalnym zadaniem i że nic nie jest naprawdę bezpieczne. Najlepsze, na co możesz liczyć, to maksymalne ograniczenie ryzyka przy jednoczesnym utrzymaniu rentownego modelu biznesowego. Główne zagrożenia można podzielić na następujące kategorie:

• ujawnienie informacji, zazwyczaj nieumyślne;

• ataki socjotechniczne na pracowników;

• Atak komputerowy i sieciowy;

• Słabe bezpieczeństwo fizyczne;

• Zbieranie informacji fizycznej.

Przynajmniej nie każda organizacja może liczyć na wszystkie te zagrożenia po równo. Dla organizacji ważna jest ocena poziomu ryzyka, ponieważ tylko wtedy mogą podjąć kroki w celu jego ograniczenia. Uświadomienie sobie, że ochrona firmy i jej interesów przed wszystkimi zagrożeniami może być trochę zniechęcająca, jak przygotowywanie się do bitwy. W pewnym sensie jest to jednak właściwy sposób myślenia o bezpieczeństwie: zrozumienie wroga i przewidywanie jego ataków; zrozum swoje słabości i staraj się je minimalizować. W tym rozdziale skupiono się na analizie zagrożeń z perspektywy biznesu. Biorąc pod uwagę powyższe punkty, co można zrobić, aby zmniejszyć to ryzyko? Jak możemy ograniczyć ujawnianie informacji i zapobiegać szkodliwym atakom socjotechnicznym? Jakie kroki można podjąć, aby zabezpieczyć komputery i sieci przed atakiem? Nie ma panaceum na bezpieczeństwo ani magicznej pigułki, ale to są rzeczy, o których musisz pomyśleć.

Zrozumienie źródeł ujawniania informacji

Jednym z największych problemów związanych z bezpieczeństwem, jakie może napotkać organizacja, jest próba kontrolowania przepływu informacji. Informacja to potęga i w niewłaściwych rękach może zostać wykorzystana w ataku. Organizacja powinna dążyć do zminimalizowania ujawnienia informacji i wpływu, jaki będzie miało przypadkowe narażenie. Pierwszą rzeczą, jaką robi atakujący po zidentyfikowaniu celu, są badania. Badania te obejmują głównie otwarte i publiczne źródła informacji (pamiętaj, że 90% informacji jest publicznie dostępnych). W dobie internetu możliwe jest zbudowanie relatywnie pełnego profilu ofiary bez wychodzenia z domu. Jeśli próbujesz chronić swoją firmę lub organizację, pomyśl o korporacyjnym szpiegu: jakie informacje byłyby dla Ciebie przydatne? Gdzie byś tego szukał? Dużo o tym rozmawiałem z perspektywy atakującego, ale jeśli chodzi o bezpieczeństwo, słabym ogniwem w każdym łańcuchu są zawsze ludzie. Większość ludzi nie ma pojęcia o bezpieczeństwie, zwykle dlatego, że nie doceniają natury ryzyka lub ryzyko w ogóle istnieje. W związku z tym, gdy poruszysz ten temat i zakwestionujesz brak świadomości pracownika w zakresie bezpieczeństwa lub naruszenie polityki bezpieczeństwa, jego lub jej reakcja jest zwykle zdumiona niezrozumieniem lub oburzeniem. Chociaż firma ma pewien stopień kontroli nad informacjami, które z niej wyciekają, ma bardzo niewielką kontrolę nad tym, którzy pracownicy zdecydują się ujawnić o sobie i, jak powiedziałem na wstępie, większość ujawnień informacji jest nieumyślna. Ujawnienie informacji może przybierać niemal każdą formę, ale te same problemy często się pojawiają i to właśnie omówię w tej sekcji. Na przykład serwisy społecznościowe zostały omówione w rozdziale 6 jako realny sposób gromadzenia informacji o celach, ale innymi winowajcami są strony internetowe (zarówno

firmowe, jak i osobiste) oraz wszelkie formy komunikacji, w których możesz nie być do końca pewien, z kim się komunikujesz na przykład za pomocą IRC lub komunikatorów internetowych.

Sieci społecznościowe i zawodowe

Praktycznie każdy jest obecny w Internecie, niezależnie od tego, czy jest to strona MySpace, Facebook czy profesjonalna alternatywa, taka jak LinkedIn. Co dziwne, wiele osób narzeka na kamery CCTV, ID karty i inne naruszenia prywatności sponsorowane przez rząd są największymi ekshibicjonistami, jeśli chodzi o takie strony. Witryny sieciowe są źródłem informacji, z których część może narazić ludzi na niebezpieczeństwo. Jednym z problemów jest to, że takie witryny promują „kontakty" lub „znajomych" jako status: im więcej masz, tym lepiej. Ja też jestem tego winny, akceptuję wszystkie zaproszenia do mojego profilu LinkedIn, więc wydaje mi się, że naprawdę połączonych, gdy w rzeczywistości znam lub spotkałem tylko ułamek tych osób. Jaka jest szkoda? Cóż, po pierwsze, jeśli ktoś jest na Twojej liście znajomych, ludzie zakładają, że go znasz i mogą użyć tego połączenia, aby przypisać komuś większe zaufanie, niż na to zasługują. Po drugie, nawet profile prywatne są zwykle widoczne dla twoich znajomych, a na LinkedIn (i jego odpowiednikach) zazwyczaj zawiera on r´esum´es. Posiadanie r´esum´e online jest niezwykle wygodne dla osób poszukujących pracy i pracodawców (nie wspominając o najgorszej formie „konsultanta ds. Rekrutacji"). Są jednak bardzo przydatne dla innych osób: windykatorów, prywatnych detektywów i inżynierów społecznych. Możliwe jest szybkie zlokalizowanie wielu osób, które pracują dla firmy docelowej; To sprawia, że wymazywanie nazwiska jest bardzo proste, szczególnie w dużych międzynarodowych firmach, w których pracownicy nawet na podobnych stanowiskach mogą się nie znać. Niejednokrotnie, gdy przeprowadzałem atak socjotechniczny, tworzyłem fałszywe profile LinkedIn i użyłem ich jako jedynej formy wiarygodności, kiedy przedstawiałem się innym. Mój prawdziwy profil LinkedIn został wykorzystany do zbadania mnie podczas rozmowy kwalifikacyjnej lub nowego klienta; w miarę rozwoju profili jest dość dokładny, ale bardzo rzadko weryfikowany. Można to doprowadzić do skrajności. Profile LinkedIn można tworzyć dla wielu pracowników tej samej „firmy". Nie jest to trudne do wykonania w przekonujący sposób. Dlatego zbytnio wierzymy w to, co ludzie o sobie piszą, to zły pomysł. Jednak większym problemem jest to, jak wpłynie to na organizację. Czasami najbardziej niewinne komentarze na blogu mogą ujawnić poufne informacje lub przedstawić firmę w złym świetle. Było wiele przypadków, w których poufne informacje o produktach sprzed embargo były dostatecznie napomykane w Internecie, aby skłonić konkurentów i dziennikarzy do zwrócenia uwagi - luźne usta toną statki i tak dalej. Było również kilka przypadków, w których pracownicy byli zwalniani za mówienie nieprzyjemnych rzeczy o ich pracodawcy. Chociaż uważam, że to niesprawiedliwe, przynajmniej firma była świadoma tego, co o niej napisano. Jeśli wdrażając zabezpieczenia, musisz radzić sobie z takimi incydentami za pomocą środków dyscyplinarnych, naprawdę już straciłeś. Znacznie lepiej, jeśli pracownicy wiedzą, że ich umowy o zachowaniu poufności obejmują internet i że jest to egzekwowane w polityce bezpieczeństwa. Zachęcaj pracowników do zwięzłości podczas publikowania w Internecie r´esum´es, które każdy może przeczytać. (Bardziej szczegółowe zawsze mogą przesłać później.) Zaakceptuj fakt, że Twoi pracownicy w pewnym momencie przejdą dalej i dbaj o profesjonalizm. W związku z tym gorąco zachęcam firmy, aby w miarę możliwości nie współpracowały z agencjami rekrutacyjnymi. Wołają znikąd, oczekują wszelkiego rodzaju informacji, a ty nie masz pojęcia, kim oni są. (Rekruter jest często idealnym przebraniem dla inżyniera społecznego). Korporacje powinny same zamieszczać ogłoszenia na odpowiednich forach; to praca dla działu personalnego - oszczędza pieniądze i zapewnia spokój. Serwisy społecznościowe działają poprzez pozyskiwanie jak największej liczby użytkowników na wspólnej platformie. Jest to luka sama w sobie; jeśli osoba atakująca może złamać prawowity profil jednego użytkownika, jest w idealnym położeniu do przeprowadzenia ataków wymagających pewnego stopnia zaufania (tj. koni trojańskich) wobec innych połączeń.

Nie można uniemożliwić pracownikom prowadzenia prywatnego życia i publikowania w Internecie wszystkiego, co tylko zechcą. Jednak specjaliści do spraw bezpieczeństwa powinni jasno uświadomić pracownikom, że serwisy społecznościowe i profesjonalne mogą być nadużywane przez osoby atakujące. Polityka bezpieczeństwa powinna sugerować, że personel nie akceptuje kontaktów od osób, których nie znają. Podejrzana jest prywatność profili na Facebooku i MySpace. W szczególności MI5 w Wielkiej Brytanii wydaje się być zainteresowana tymi witrynami: ministrowie ujawnili , że rozważają komunikaty policyjne wysyłane za pośrednictwem witryn takich jak MySpace i Facebook, a także plany przechowywania informacji o każdej rozmowie telefonicznej, e-mailu i wizycie w Internecie wykonanej przez wszystkich. w Zjednoczonym Królestwie. Może pracownicy ochrony chcą po prostu uzasadnić swój czas na blogowanie. Ale wątpię w to.

Witryny firmowe

To niefortunny fakt, że zdecydowana większość informacji wykorzystywanych przeciwko organizacji pochodzi z organizacji. Wchodząc na firmową stronę internetową można zwykle uzyskać zaskakującą ilość danych. W tym celu przydatne mogą być publiczne witryny firmowe, jednak witryny publiczne często nie są najgorszymi winowajcami. Często zdarza się, że witryny prywatne (a przynajmniej te, które powinny być prywatne) są konfigurowane do użytku pracowników. Zazwyczaj znajdują się one w tej samej podsieci internetowej (lub przynajmniej w tej samej domenie internetowej) co systemy publiczne, ale nie są publicznie reklamowane w przekonaniu, że osoba atakująca nie będzie w stanie ich znaleźć. W rzeczywistości jedną z pierwszych rzeczy jaką atakujący może zidentyfikować publiczne witryny internetowe. Ponieważ zakresy internetowe nie są informacjami prywatnymi i można uzyskać do nich dostęp za pośrednictwem publicznych baz danych, takich jak RIPE lub ARIN, informują one atakującego, jakie adresy IP posiada firma. Dzięki tym informacjom osoba atakująca może po prostu przeskanować te adresy w poszukiwaniu serwerów internetowych. Aby się przed tym zabezpieczyć, upewnij się, że jedynymi serwerami sieciowymi w Twojej strefie zdemilitaryzowanej (DMZ) są publicznie dostępne systemy, które nie zawierają poufnych danych. Prywatne informacje, do których pracownicy lub partnerzy muszą mieć dostęp, powinny być dostępne przez VPN. Nie zawsze jest to możliwe, więc jako kopia zapasowa użyj silnego uwierzytelniania na serwerach WWW i konwencji nazewnictwa, która nie określa przeznaczenia danego serwera. Na na przykład adres dmz0112.companyx.com jest prawidłowy, ale hr.companyx.com nie.

Prywatne witryny internetowe

Osobiste witryny internetowe to kolejny problem, ponieważ ludzie lubią umieszczać w Internecie wiele informacji o sobie. Często zawiera to szczegóły dotyczące ich pracy. Wielu pracodawców (słusznie) zauważy, że nie ma w tym nic złego i prawdopodobnie zachęciłoby pracowników do pokazania, że są dumni z tego, gdzie pracują. Czasami jednak najbardziej nieszkodliwe informacje mogą być przydatne dla atakującego. Po prostu wymień, co robisz i dla kogo może być punktem wyjścia do ataku socjotechnicznego. Jak więc znaleźć równowagę między najlepszymi praktykami w zakresie bezpieczeństwa a jawna paranoja? Najlepszą polityką jest zachęcanie pracowników do jak największego oddzielania pracy od życia domowego, a to i tak jest zdrowe.

USENET

Był taki czas (i to były dobre czasy), kiedy wszystkie dyskusje, które miały miejsce w Internecie, odbywały się na USENET lub IRC. Najwyraźniej czasy się zmieniły w przypadku forów internetowych, ale przestrzeganie zasad bezpiecznego postępowania w Internecie stało się proporcjonalnie ważniejsze wraz z rozwojem nowych technologii. Zwróciłem szczególną uwagę na USENET, ponieważ jest to z natury niebezpieczne miejsce do publikowania praktycznie wszystkiego:

• Wszystko, co wpisujesz, może być powiązane z Twoim adresem IP, prowadząc z powrotem do Ciebie, nawet jeśli nie używasz Twojego prawdziwego imienia i nazwiska lub adresu e-mail.

• To całkowicie otwarte forum: każdy może zobaczyć, co publikujesz.

• Archiwa zwykle przechowują posty w nieskończoność i umożliwiają ich przeszukiwanie.

Wszystko to oznacza, że bezmyślny komentarz, jaki ktoś wygłosił na temat swojego szefa, pozostanie tam na zawsze. Osoba, która opublikowała komentarz, może nie być identyfikowalna, ale adres IP (który, mamy nadzieję, nie pochodzi z pracy), z którego został opublikowany, z pewnością jest. A tak poważnie, bezpieczeństwo nie powinno zezwalać na wysyłanie postów do USENET-u z sieci firmowej, chyba że jest ograniczone do kilku grup, które mogą tego potrzebować do określonych projektów. Zbyt łatwo jest prześledzić konkretne pytania i uwagi do firmy. Poza tym obowiązuje ta sama rada, co w przypadku portali społecznościowych: uważaj na to, co jest publikowane i upewnij się, że personel robi to samo. To, co dziś piszesz, prawdopodobnie zostanie gdzieś zarchiwizowane przez dłuższy czas.

IRC i komunikatory internetowe

IRC to zupełnie inna kategoria ryb i moim głównym zastrzeżeniem jest to, że jego ruch jest nieszyfrowany, chociaż jest również popularnym wektorem ataku trojanów i innego złośliwego oprogramowania. (Nawet jeśli korzystasz z zaszyfrowanego kanału, nie jesteś bezpieczny). W związku z tym nie nadaje się on do użytku jako narzędzie komunikacji biznesowej. Jednak wiele firm używa go jako takiego. Nie ma nic złego w IRC, jeśli jest wdrożony na serwerze wewnętrznym, a połączenia są ograniczone do tych przez Internet przez VPN. Jeśli VPN nie wchodzi w grę, tunele SSH są doskonałą alternatywą. Osoba atakująca może ustalić na podstawie osobistych witryn internetowych, które kanały IRC są popularne wśród określonych pracowników, zapewniając w ten sposób łatwą drogę do ich oczyszczenia. Korzystanie z publicznych kanałów IRC nie jest tak popularne jak kiedyś. W dzisiejszych czasach czat błyskawiczny i sieci społecznościowe rządzą grzędą i nie są o wiele bezpieczniejsze. Praktycznie wszystkie systemy wiadomości błyskawicznych używają niezaszyfrowanych protokołów - chociaż można to złagodzić za pomocą różnych dodatków. Wiadomości błyskawiczne omówiłem w rozdziale 10

Ataki inżynierii społecznej

Zakładając, że przeczytałeś Część 4, prawdopodobnie doszedłeś do wniosku, że są to najtrudniejsze ataki do obrony. Niestety to prawda. Istnieją jednak dwa główne kroki, które możesz podjąć, aby zmniejszyć ryzyko:

• Egzekwuj odpowiednią politykę bezpieczeństwa - procedury dokumentowania mogą zminimalizować ryzyko w danym obszarze. Jeśli nie jest to możliwe dla jednej osoby aby uwolnić wrażliwy materiał, to ogromna ilość inżynierii społecznej ataki można powstrzymać. Upewnij się, że przynajmniej część osób jest zaangażowana w ten proces mają naturalnie sceptyczny umysł.

• Szkolić personel - upewnić się, że pracownicy są świadomi zagrożeń, na jakie napotykają, oraz typowych wektorów ataków. To jest pierwszy i najważniejszy punkt. Osoby, które nie są świadome istnienia ryzyka, nie mają szans się przed nim bronić. Łatwo jest pisać komentarze typu „Wyedukuj swój personel przed atakami socjotechnicznymi!" Podejrzewam jednak, że szukasz czegoś więcej. Szkolenie w zakresie świadomości bezpieczeństwa to znacznie więcej niż zwykłe mówienie użytkownikom, aby nie podawali swoich haseł. Kevin Mitnick (słynny haker i inżynier społeczny) niejednokrotnie stwierdził, że ani razu nikogo nie poprosił o podanie hasła. Podczas szkolenia pracowników należy odnieść się do następujących obszarów jako punktu odniesienia:

• Zrozumienie zagrożenia.

• Zrozumienie, co ma wartość.

• Rozpoznawanie i radzenie sobie z potencjalnym atakiem.

Zrozumieć zagrożenie

To faktycznie najtrudniejsza przeszkoda do pokonania. Koncepcja ukierunkowanych ataków hakerskich i szpiegowskich na biznes wykracza poza sferę doświadczenia większości ludzi i w związku z tym jest trudna do zrozumienia. Mentalność „to nie może się zdarzyć tutaj" lub „to mi się nie przydarzy" to podejście, które większość ludzi musi stracić. Dobrym sposobem na przeszkolenie personelu jest myślenie o przykładowych scenariuszach, które odnoszą się bezpośrednio do Twojej firmy; jak ktoś mógłby cię zaatakować i jakie byłyby jego atuty docelowe? Rozdział 4 wyjaśnia podstawowe zasady przeprowadzania tych ataków. Sesje szkoleniowe dotyczące bezpieczeństwa, które zachęcają do ćwiczeń polegających na odgrywaniu ról w celu wykazania zagrożeń, są skutecznymi technikami edukacyjnymi. Aby skorzystać z tego, co omówiliśmy wcześniej z perspektywy osoby atakującej, należy wyjaśnić następujące podstawowe kwestie:

• Poufne dane są poufne, a hasła są danymi osobowymi - wykazanie, dlaczego istnieją zasady bezpieczeństwa, pozwala pracownikom dostrzec, że nie jest to jedynie ćwiczenie paranoi lub biurokracji. W cotygodniowych wiadomościach pojawia się mnóstwo informacji dotyczących incydentów bezpieczeństwa. Prezentacje dla pracowników powinny zawierać niedawne i istotne ataki, a także konsekwencje finansowe i prawne dla danych firm.

• Przyjaciele nie zawsze są tym, na kogo się wydają - kluczowym problemem jest nauczenie pracowników, aby nie pokładali zaufania tam, gdzie nie należy. Osiągnięcie równowagi między bezpieczeństwem a codzienną rzeczywistością skutecznego i wydajnego prowadzenia firmy nie zawsze jest łatwe. Na przykład inżynier społeczy może twierdzić, że jest starszym członkiem zespołu zarządzającego, który pozyskuje informacje za pomocą zakładanego upoważnienia, ale na co dzień starsi członkowie zespołu zarządzającego prawdopodobnie szukają pracowników, którzy nigdy ich nie spotkali. Dlatego świadomość bezpieczeństwa ma kluczowe znaczenie na wszystkich poziomach działalności. W takich okolicznościach nawet menedżerowie powinni spodziewać się wyzwania.

• Pozory mogą mylić - mundury są tanie. Omawialiśmy scenariusze wcześniej, w których mechanizmy bezpieczeństwa były omijane przez napastnika w mundurze doręczyciela lub kuriera. Ponieważ tacy ludzie przez cały czas wchodzą i wychodzą z firm, są zwykle ignorowani, co jest oczywiście powodem, dla którego atak działa tak dobrze. Personel (zwłaszcza personel recepcji) musi zrozumieć, że każdy może nabyć takie mundury i ulepszyć je, tworząc lub kopiując logo na drukarce atramentowej. Ponownie wszystko, czego potrzeba, to odpowiednia identyfikacja przy barierze organizacyjnej. Polityka bezpieczeństwa powinna upewnić się, że doręczyciele, których się nie oczekuje, nie wchodzą do środka. Osoby, które nie mogą się odpowiednio zidentyfikować, nie wchodzą do środka. Po zidentyfikowaniu gości należy odprowadzić do miejsca docelowego lub spotkania przez gospodarza w recepcji. Kurierzy nigdy nie powinni mieć możliwości opuszczenia recepcji, bez względu na instrukcje.

Zrozumienie, co ma wartość

Jedną z przesłanek, których używają inżynierowie społeczni w celu uzyskania informacji, jest celowanie w postrzegany brak wartości, jaki może mieć dana informacja. Dobrym przykładem jest książka telefoniczna; nie jest to ściśle tajne. Każdy w firmie ma kopię, więc jaką możliwą wartość miałaby dla atakującego? Taka postawa jest często wykorzystywana nawet wtedy, gdy ofiara może mieć ukryte

podejrzenia co do dzwoniącego. Książka telefoniczna ma ogromną wartość w ataku socjotechnicznym, jak pokazano w Części 4.

Podaj przykłady różnych zasobów i informacji w organizacji, które miałyby namacalną wartość dla atakującego. Oczywiście będzie się to różnić w zależności od firmy, ale wspólne tematy obejmują:

• Informacje o personelu - może to być wszystko, od (obecnie wszechobecnej) książki telefonicznej po rejestry zasobów ludzkich.

• Dane zastrzeżone - to poufne dane odnoszące się bezpośrednio do podstawowych interesów biznesowych firmy. Wartość tego powinna być oczywista - problem polega na utrzymaniu jej własności. Jedną z prostych zasad, które powinieneś egzekwować w swojej organizacji, jest zapewnienie, że Twoi pracownicy blokują swoje stacje robocze, nawet jeśli odsuwają się na chwilę. Kiedyś pracowałem w miejscu, które traktowało to tak poważnie, że każdy, kto znalazł odblokowany komputer, mógł go użyć do wysłania e-maila do reszty firmy z informacją o tym fakcie. Jest to potwornie żenujące i nikt nie popełnił tego samego błędu dwa razy.

• Dokumentacja finansowa - wartość tutaj może nie być od razu oczywista; w końcu na koniec dnia kogo obchodzi, jakie pieniądze trafiają na konta, a jakie z nich wychodzą? Tego rodzaju informacje są niezwykle cenne w rękach osób, które mogą je zinterpretować, na przykład osób handlujących poufnymi informacjami i tych, którzy chcą wykorzystać nadchodzącą fuzję lub przejęcie. Jeśli finanse za następny kwartał nie wyglądają zbyt dobrze (są to informacje sprzed embargo), nadal można osiągnąć zyski, skracając akcje firmy, czego - mówiąc krótko - należy unikać. I odwrotnie, dane finansowe, które wyciekły, mogą obniżyć ceny akcji i mogą być wykorzystane jako część ataku „krótkiego i zniekształcającego", powszechnej (choć nielegalnej) taktyki podczas bessy.

• Komunikacja - w firmie zatrudniającej więcej niż kilkaset pracowników nierzadko zdarza się, że popełniane są błędy w listach dystrybucyjnych. Nie jest też niemożliwe, aby osoba atakująca spowodowała taki błąd, manipulując pracownikami w celu dodania ich do listy lub przekazania wiadomości. Menedżerowie, którzy zostawiają swoje e-maile do obsługi sekretarek, są szczególnie narażeni na tego rodzaju ataki. Bardziej odważne ataki polegają na podszywaniu się pod pracowników i proszeniu o przesłanie wszystkich faksów na inny numer.

• Zasoby fizyczne - nie zapomnij o zwykłym złodzieju! Nie ma nic bardziej frustrujące niż tworzenie polityki bezpieczeństwa informacji aby radzić sobie ze szpiegami korporacyjnymi i hakerami tylko po to, aby ktoś wszedł i ukradł 20 laptopów. To naprawdę żenujące.

Rozpoznawanie zagrożeń i postępowanie z nimi

Celem szkolenia personelu jest przede wszystkim zapobieganie incydentom bezpieczeństwa - „Stała czujność!", Jak powiedziałby Szalonooki Moody. Jeśli jednak pracownicy podejrzewają, że są celem, jak powinni zareagować? Istnieją dwie możliwości:

• Powtórzenie linii firmowej - „Nie, proszę pana, nie mogę pozwolić na uzyskanie tych informacji bez weryfikacji przez telefon" lub „Obawiam się, że nikt nie wejdzie do budynku bez umówionego terminu". Nieważne. Jest to z pewnością bezpieczniejsza opcja. Nie wywiera też nadmiernej presji na Twoich pracowników. Chociaż za bezpieczeństwo odpowiada każdy, recepcjonistki nie powinny czuć się jak ochroniarze. To po prostu niesprawiedliwe. Jeśli jednak uważa się, że trwa poważny lub dobrze zorganizowany atak, możesz pójść dalej.

• Eskalacja - procedury eskalacji stosowane przez personel powinny odzwierciedlać charakter ataku. Jeśli „atakujący" jest na miejscu, należy natychmiast wezwać ochronę. Przykłady tego obejmują

sytuacje, gdy ktoś chce uzyskać dostęp do witryny, ale nie może lub odmawia identyfikacji, lub gdy ktoś jest proszony o informacje i staje się agresywny po odmowie lub prośbie o identyfikację. Jeśli podejrzewa się atak socjotechniczny za pośrednictwem poczty elektronicznej lub telefonu, sytuacja staje się bardziej skomplikowana. E-maile należy przesyłać do działu bezpieczeństwa informacji z nienaruszonymi nagłówkami, a numery telefonów należy zapisać w celu dalszego zbadania. Nigdy nie ufaj ID dzwoniącemu jako jedynemu sposobowi identyfikacji dzwoniącego: fałszowanie go jest trywialne. Poproś o numer, aby oddzwonić. Nie trzeba dodawać, że odmowę podania numeru należy traktować podejrzliwie. Każde wezwanie do udzielenia informacji z numeru zastrzeżonego powinno być traktowane podobnie. Standardową taktyką socjotechniczną w przypadku wyzwań napastnika jest wywołanie u ofiary strachu o swoją pracę. Nie powinno to zniechęcać pracowników. Każdy, kto jest uprawniony do dostępu do wrażliwych witryn lub informacji poufnych, powinien dobrze znać politykę bezpieczeństwa firmy. W praktyce należy uczyć pracowników, że udostępnianie intruzowi znacznie bardziej ogranicza karierę zawodową niż tymczasowo utrudnia komuś, kto powinien wiedzieć lepiej. Ważne jest, aby Twoi pracownicy byli w stanie wykryć ataki socjotechniczne i występowały kluczowe oznaki, na które należy uważać:

• Poczucie przymusu do ujawniania zastrzeżonych informacji lub łamania polityki bezpieczeństwa firmy;

• Niemożność znalezienia odpowiedniej osoby i poproszenia o potwierdzenie;

• pośpiech;

• Bycie podchodzącym do kogoś, kto upuszcza nazwiska i tytuły;

• Obawa spowodowania opóźnienia lub wykroczenia.

Wreszcie pracownicy powinni wiedzieć, że jeśli ktoś po prostu nie czuje się „dobrze", może kierować się swoim instynktem.

Ochrona przed monitorowaniem elektronicznym

Stosowanie elektronicznego monitorowania lub „podsłuchiwania" jest poważnym zagrożeniem, które jest znacznie bardziej rozpowszechnione, niż się powszechnie uważa. Jednak na szczęście nie jest to prosty atak do wykonania, a przynajmniej nie jest łatwy do wykonania dobrze. Sprzęt dostępny w sklepach szpiegowskich i używany przez prywatnych śledczych jest zwykle znacznie poniżej jakości dostępnej dla agencji wywiadowczych. W związku z tym stosunkowo łatwo jest zabezpieczyć się przed podsłuchiwaniem, jeśli uważasz, że masz problem i wiesz, czego szukać. Poniższa lista obejmuje niektóre oznaki, które mogą wskazywać, że jesteś pod obserwacją. Nie jest jednak wyczerpująca i żaden problem nie sugeruje, że jesteś pod obserwacją. Nie wpadaj w paranoję!

• Jesteś ofiarą włamania, ale wygląda na to, że nic nie zostało zabrane.

• Otrzymujesz urządzenie elektroniczne w prezencie, a jego pochodzenie nie jest jasne lub otrzymujesz taki prezent od sprzedawcy lub innego partnera biznesowego. Pamiętaj, „strzeżcie się Greków niosących prezenty": jest powód, dla którego to jest frazes.

• Na ścianie, suficie lub listwie przypodłogowej pojawia się nagle niewyjaśniony guzek lub przebarwienie.

• Elektryczne płyty ścienne zostały nieco przesunięte.

• Czujnik dymu, zegar, lampa itp. W Twoim biurze wygląda na lekko zakrzywiony lub ma małą dziurkę w powierzchni. Powierzchnie półodblaskowe są charakterystycznym znakiem ukrytych kamer.

• Przedmioty pojawiają się w Twoim biurze, szczególnie na biurku, ale nikt nie wie, jak się tam dostały.

• Kurz lub zanieczyszczenia są obecne na podłodze obok ściany, tak jakby ktoś wiercił, lub na podłodze widać małe kawałki płytek sufitowych lub żwir.

• Samochody dostawcze firmy telekomunikacyjnej lub innego przedsiębiorstwa spędzają dużo czasu poza budynkiem biurowym lub pojazdy serwisowe są często zaparkowane w pobliżu i wydają się być niezamieszkane (nie oznacza to, że tak jest).

• Naprawiający ludzie przychodzą do pracy, kiedy nikt do nich nie dzwonił.

• Zamki drzwi nagle zmieniają się lub przestają działać. Jest to znak, że w celu uzyskania dostępu użyto karabinków.

• Meble lekko się przesunęły i nikt nie wie dlaczego.

• Uważasz, że twoje szuflady zostały przeszukane, ale nic się nie pojawia i nic nie może zabraknąć.

• Na liniach telefonicznych słychać dziwne dźwięki lub zmiany głośności albo zauważysz szumy, trzaski lub rysy. Jest to spowodowane błędami niskiej jakości, które zakłócają lub pobierają energię z linii telefonicznej.

• Dźwięki są odtwarzane przez słuchawkę telefonu, gdy jest rozłączona.

• Twój telefon często dzwoni i nikogo nie ma, chociaż mogą występować zakłócenia lub słabe wysokie tony.

• W radiu AM / FM lub w telewizorze pojawiają się nagle dziwne zakłócenia. Błędy kupione w sklepie używają standardowych wymagań komercyjnych a kryształy kwarcu, które je napędzają, często oddalają się od nich jak zaprogramowane kanały.

Po ustaleniu, że możesz mieć problem, musisz zdecydować jak się zachować. Kusi, by wziąć sprawy w swoje ręce i samodzielnie szukać błędów. Nie. Trudno jest udowodnić, że coś jest negatywne, a jeśli przyjdziesz z pustymi rękami, nie będziesz się niczego upewniał. Istnieją komercyjne urządzenia do usuwania błędów, ponownie dostępne w sklepach szpiegowskich, ale są one prawie bezużyteczne. Każde urządzenie poniżej 1000 USD to niewiele więcej niż zabawka. Jeśli uważasz, że Twoje biuro jest podsłuchiwane lub masz podsłuchiwaną linię telefoniczną, musisz szybko sprowadzić specjalistów. Nie ulegaj pokusie zatrudniania prywatnych detektywów z dwóch powodów: nie mają oni kwalifikacji do wykonywania tego rodzaju pracy (chociaż wielu reklamuje usługi usuwania błędów) i musisz wziąć pod uwagę możliwość, że w końcu zatrudnisz osoby, które zainstalował błąd w pierwszej kolejności. Są firmy, które specjalizują się w przeciwdziałaniu zagrożeniom ze strony błędów i to są osoby, do których należy zadzwonić. Znajdź taki w swojej okolicy (nie korzystaj z komputera w biurze ani telefonu) i umów się na spotkanie poza siedzibą firmy. Przyprowadzając specjalistów do biura, zapewnij im odpowiednią ochronę. Dobra okładka to rozmowa kwalifikacyjna lub audyt finansowy, ale wybierz coś odpowiedniego i wiarygodnego. Na tym etapie nie wiesz, kto stoi za nadzorem. Jeśli to możliwe, nikomu nie mów.

Zabezpieczanie odmowy

W Części 6 omówiłem niebezpieczeństwa „nurkowania w śmietniku”. Przypomnę, w tym miejscu intruz dosłownie przegląda twoje śmieci w poszukiwaniu informacji, które pomogą sformułować lub rozszerzyć plan ataku. Chociaż zabezpieczenia przed tym mogą wydawać się oczywiste, najwyraźniej nie są lub nie byłoby problemu. Aby zmniejszyć ryzyko, jakie to stwarza, należy wziąć pod uwagę kilka rzeczy:

• Co kończy w koszu - jeśli możesz zapobiec (lub przynajmniej zmniejszyć ilość) poufnych, wrażliwych lub uprzywilejowanych informacji trafiających do kosza, wówczas fizyczne bezpieczeństwo samych śmietników staje się kwestią sporną. To powinno być twoje podejście, zanim zaczniesz myśleć o czymkolwiek innym. Wszelkie odpady papierowe zawierające informacje o klientach, wiadomości e-mail, listy telefonów itp. Należy rozdrabniać za pomocą niszczarki krzyżowej. To, jak daleko wyjdziesz poza to, zależy od Ciebie. Niektóre firmy mają zasady, które wymagają, aby wszystkie zniszczone informacje były spalane lub transportowane na lokalne wysypisko przez zaufane osoby. Jednak moim zdaniem nie jest to praktyczne. Jeśli to możliwe, unikaj wyrzucania nośników elektronicznych do śmieci, ale wszystkie wyrzucane nośniki powinny zostać oczyszczone kryptograficznie przed utylizacją.

• Zabezpieczenie śmietnika - Idealnie, pojemniki na śmieci powinny być zabezpieczone, chociaż nie jest to tak łatwe, jak się wydaje i dalekie od praktycznego. Do śmietników muszą mieć dostęp przynajmniej dwie strony: ekipa sprzątająca i ekipa zbierająca. Jeśli śmietniki są zamknięte, tym osobom należy wydać klucze. Wymaga to skorzystania z dedykowanej firmy zajmującej się odpadami, która specjalizuje się w bezpiecznej zbiórce; takie firmy istnieją (i dostarczają własne kontenery), ale spodziewają się zapłacić wyższą cenę.

• Lokalizacja - jest to najłatwiejszy i najbardziej oczywisty środek zaradczy w nurkowaniu na śmietniku. Celem jest, aby ryzyko bycia złapanym przekroczyło potencjalną nagrodę w postaci znalezienia informacji wartych kradzieży. Jeśli twoje śmietniki znajdują się za zamkniętymi bramami i dobrze w granicach firmy, intruz musi popełnić przestępstwo, aby po prostu otworzyć śmietnik. W dobrze oświetlonym obiekcie z dobrym środkiem odstraszającym, takim jak kamery i nocne patrole, większość ludzi pomyśli dwa razy. Z drugiej strony wiele firm przechowuje swoje śmietniki w lokalizacjach, które technicznie są poza ich terenem, co oznacza, że możesz zrobić bardzo niewiele, aby powstrzymać napastników - zarówno fizycznie, jak i prawnie. Nurkowanie w śmietniku to jedna z pierwszych rzeczy, które prywatny detektyw, inżynier społeczny lub dziennikarz podejmie podczas profilowania Twojej witryny lub personelu - nie ułatwiaj im tego.

Ochrona przed tailgating i łopatką

Tailgating i bark surfing to dwa ataki, które są bardzo łatwe do wykrycia, jeśli personel jest świadomy zagrożenia i nie zdaje sobie z tego sprawy. Te ataki często kończą się sukcesem, ponieważ ludzie zwykle nie chcą rzucać wyzwania innym. Wykonałem wystarczająco dużo ataków typu tailgating, aby wiedzieć, że przez większość czasu najgorsze, co będziesz cierpieć, to surowy wygląd, a nawet to jest wyjątkiem od reguły. Często ludzie otwierają ci drzwi, jeśli grzecznie ich poprosisz. Istnieją dwa sposoby zapobiegania atakom tailgating:

• Edukuj pracowników - Uświadomienie personelowi zagrożenia jest podstawą każdej strategii bezpieczeństwa (jak powtarzałem w tej książce). Jeśli ktoś podąża za tobą przez drzwi, szczególnie jeśli wydaje się, że czekał obok nich lub gdy zjawia się znikąd, nie bój się poprosić o pokazanie przepustki lub plakietki. Jeśli jest to obowiązkowe w ramach polityki bezpieczeństwa witryny, ludzie będą mieli mniejszy problem z przestrzeganiem tego. Nikt nie chce czuć się jak palant, więc to postawi wszystkich na równej stopie.

• Wdrożenie fizycznej kontroli dostępu - możliwe jest zainstalowanie fizycznych kontroli, takich jak pułapki na ludzi, które uniemożliwiają śledzenie ogonów. Te stają się coraz częstszym widokiem na granicach dużych firm. Problem polega jednak na tym, że ataki typu tailgating zwykle nie występują na granicy, ale w samej witrynie. Po przekroczeniu granicy jest to całkowicie niepraktyczne, aby mieć wszędzie taką formę kontroli dostępu, a większość witryn wdraża jakąś formę tokena zbliżeniowego, aby zapobiec nieautoryzowanemu dostępowi. Uzyskanie fizycznego dostępu do dowolnej witryny nigdy nie jest tak trudne, jak można by sobie wyobrazić, więc znacznie lepiej jest upewnić się, że

personel rozumie ryzyko (i jest przygotowany do rzucenia wyzwania potencjalnym intruzom), niż polegać na jakimkolwiek fizycznym zautomatyzowanym systemie.

Surfowanie przez ramię może być problemem wszędzie tam, gdzie używane są hasła lub kody dostępu, np. Logowanie do komputerów czy otwieranie drzwi. Ta sama rada ma zastosowanie w tym przypadku, co w przypadku tailgating: należy uważać na otoczenie podczas obchodzenia się z poufnymi informacjami, zwłaszcza hasłami. Personel nigdy nie powinien bać się prosić kogoś o odwrócenie wzroku podczas wpisywania hasła lub zakrycie klawiatury podczas wpisywania kodu do drzwi. Jeśli uważają, że ktoś aktywnie próbuje zdobyć hasła lub kody dostępu, należy ich zachęcić do natychmiastowego wezwania ochrony. Wiele haseł zostaje skradzionych nie przez kogoś, kto obserwuje, jak wpisuje je użytkownik, ale przez kogoś, kto czyta je na biurkach innych osób. Klisza hasła na notatce przyklejonej do czyjegoś monitora jest banałem nie bez powodu: ludzie to robią. Powinno to stanowić naruszenie polityki bezpieczeństwa firmy.

Wykonywanie testów penetracyjnych

Regularne testy penetracyjne są krytycznym elementem ogólnej strategii bezpieczeństwa. Testowanie daje dobre wyobrażenie o tym, jak silna jest Twoja pozycja w zakresie bezpieczeństwa i ile pracy musisz wykonać. To, co przetestowałeś (i jak często) jest unikalne dla twojej organizacji i twoich indywidualnych preferencji, ale ogólnie mówiąc testy penetracyjne dzielą się na dwie odrębne kategorie: fizyczną i elektroniczną (przy czym elektronika jest zdecydowanie najpopularniejsza).

Testy fizyczne

Celem testów fizycznych jest określenie:

• skuteczność kontroli bezpieczeństwa granic;

• skuteczność wewnętrznych środków kontroli bezpieczeństwa;

• podatność personelu na manipulację;

• podatność organizacji na wyciek informacji;

• skuteczność wdrożonej polityki bezpieczeństwa;

• ogólne zagrożenie, na jakie organizacja napotyka atak fizyczny.

Prawidłowo wykonany test penetracji fizycznej może wiele powiedzieć o Twojej słabości. Zwykle pokaże ci, że jesteś podatny na ataki w wielu obszarach i dlatego nie ma sensu angażować się w test z czysto spekulatywnych powodów, ale mając na uwadze konkretne cele. Dobre przykłady to:

• zidentyfikowanie słabych punktów w określonych obszarach;

• testowanie implementacji niedawno wdrożonych systemów lub procedur;

• w ramach regularnego audytu w celu sprawdzenia zgodności z polityką bezpieczeństwa;

• niezależne zweryfikowanie istnienia zagrożeń, o których wiesz lub podejrzewasz, że występują (jest to zwykle konieczne, aby uzasadnić zwiększenie budżetu);

• do symulacji ataku określonej grupy lub kategorii zagrożeń. Są one zwykle bardzo specyficzne dla organizacji.

Fizyczne testy penetracyjne to stosunkowo nowa oferta konsultingowa (przynajmniej w sektorze komercyjnym), więc może być trudno zdecydować, z kogo skorzystać. Trudność tę komplikuje fakt, że

charakter pracy może sprawiać, że raporty są dość subiektywne i ulotne. Elektroniczne testy penetracyjne borykają się z tymi samymi problemami, ale jest to bardziej dojrzała branża z jasno określonymi normami, wzorcami i klasami podatności. O wiele trudniej jest ocenić kompetencje i doświadczenie testerów penetracji fizycznej. Byłoby niewłaściwe wydawanie konkretnych zaleceń lub omawianie firmy, dla której pracuję, ale przynajmniej powinieneś zwrócić uwagę na następujące kwestie:

• Sprawdzone doświadczenie - firmy powinny być w stanie wykazać się sukcesem w realizacji zadań tego rodzaju. Wiele firm testujących bezpieczeństwo ogłasza teraz testy fizyczne na swoich stronach internetowych jako część swojego portfolio konsultingowego. Nie oznacza to, że faktycznie coś zrobili w przeszłości. Zawsze pytaj o referencje. Każda renomowana firma z solidnym doświadczeniem będzie w stanie dostarczyć przynajmniej dwa referencje dające się zweryfikować. Jeśli jesteś zaskoczony odpowiedzią, że nie można ich dostarczyć „ze względów bezpieczeństwa", natychmiast zakończ rozmowę.

• Udokumentowana metodologia - jest to absolutnie krytyczne. Metodologia nie musi mieć imponującej nazwy, ale musi być powtarzalna i dokładna. Każda firma, która mówi Ci, co robi, jest czarną sztuką i nie może zostać udokumentowana lub ponownie nie będzie o tym rozmawiać „ze względów bezpieczeństwa", marnuje Twój czas (i chce zmarnować Twoje pieniądze). Bez metodologii test nie może być powtarzalny i dlatego jest bez znaczenia.

• Szacunek w branży - każdy może stworzyć stronę internetową i nazwać siebie, jak chce, ale prawdziwi profesjonaliści się wyróżniają. Zobaczysz, jak prowadzą wykłady na imprezach i targach, publikują badania i artykuły, a nawet piszą książki. Profesjonaliści to ludzie, do których zwracają się media, gdy potrzebują komentarzy. Specjaliści ds. Bezpieczeństwa nie boją się zajęć pozalekcyjnych i nie będziesz musiał daleko szukać, aby wczuć się w ludzi, z którymi masz do czynienia.

Testowanie elektroniczne

Ta bardziej klasyczna forma testów penetracyjnych służy do określania podatności systemów komputerowych, sieci i aplikacji na atak elektroniczny zazwyczaj (ale nie wyłącznie) z Internetu. Oczywiście organizacja, która ma zamiar rozważyć fizyczne testy penetracyjne, powinna już przeprowadzić odmianę elektroniczną. Osoba atakująca musi być poważna, aby wejść do obiektu, ale każdy, gdziekolwiek, może dla kaprysu sondować hosty z dostępem do Internetu ze znacznie mniejszą szansą na złapanie. Obecnie termin „testy penetracyjne" w odniesieniu do komputerów jest używany błędnie, ponieważ bardzo niewiele osób faktycznie chce tej usługi. Większość prac wykonywanych w tej dziedzinie to w rzeczywistości „audyt bezpieczeństwa" i niekoniecznie jest to zła rzecz. Testy penetracyjne (lub hakowanie etyczne) polegają na znajdowaniu błędów i uzyskiwaniu dostępu w taki sam sposób, jak atakujący, podczas gdy audyt polega po prostu na wyszukiwaniu i raportowaniu wszystkich luk w testowanych systemach. Oczywiście ta ostatnia jest znacznie dokładniejsza i niewątpliwie ma lepszy stosunek jakości do ceny. Często te dwie usługi są łączone, z testem penetracyjnym po audycie, aby jasno wykazać podatność, chociaż nie zawsze jest to konieczne. Testy penetracyjne lub audyt bezpieczeństwa są drogie, więc dokładnie zastanów się, gdzie ćwiczenie będzie najbardziej wartościowe. Niektóre obszary do przemyślenia i informacje obejmują:

• Bezpieczeństwo granic - jest to test infrastruktury pomiędzy Twoją siecią wewnętrzną a Internetem. Intruz uzyskujący dostęp do systemów wewnętrznych to najgorszy scenariusz, więc Twoja granica musi być bezpieczna.

• Strefa zdemilitaryzowana (DMZ) - są to zazwyczaj najbardziej narażone serwery, ponieważ ich zadaniem jest świadczenie usług w Internecie.

• Podsieci wewnętrzne - zagrożenie dla systemów informatycznych nie zawsze pochodzi z Internetu, ale ze strony niezadowolonych pracowników i szpiegów przemysłowych, którzy przeniknęli do firmy. Wiele organizacji stosuje obecnie „wewnętrzne testy penetracyjne", nawet jeśli jest to trochę mylące.

• Aplikacje - jednym z obecnie najczęściej spotykanych wektorów ataków są aplikacje internetowe firmy mające dostęp do Internetu. Są ku temu trzy powody. Zwykle nie podlegają one audytowi również infrastruktury, ponieważ testowanie aplikacji wymaga specjalistycznej wiedzy programistycznej wykraczającej poza tę, którą posiada tester sieci. Luki w zabezpieczeniach są zwykle głębsze niż te, które mogą być automatycznie wykorzystywane przez robaki internetowe - co oznacza, że mogą pozostawać uśpione przez jakiś czas. Wreszcie, z powodu typowych błędów w kodowaniu i złej konfiguracji zaplecza bazy danych, osoba atakująca może wydobyć wiele poufnych informacji. Dobrze jest zlecić audyt aplikacji internetowych zespołom specjalizującym się w tej dziedzinie.

Rady dotyczące mądrego wyboru firmy testującej są tutaj równie istotne. Istnieje szereg akredytacji, które mają bezpośrednie zastosowanie do elektronicznych testów penetracyjnych. Kilka z nich omówiono w dodatkach, chociaż nie zatrudniłbym nikogo wyłącznie na tej podstawie. Nie bój się zaprosić potencjalnego zespołu na spotkanie i wypytać go o ich przeszłość i doświadczenie. Testy penetracyjne to poważna sprawa i chcesz mieć pewność, że są przeprowadzane kompetentnie.

Moja ostatnia rada jest prosta: test penetracyjny (fizyczny lub elektroniczny) to tylko migawka w czasie. Nie gwarantuje, że będziesz bezpieczny w przyszłym miesiącu (a nawet w przyszłym tygodniu). Testowanie tylko daje wyobrażenie o tym, gdzie się teraz znajdujesz. Nawet jeśli twoja infrastruktura komputerowa a aplikacje się nie zmieniają, może zostać opublikowany nowy błąd oprogramowania, który uczyni cię bardzo podatnym na ataki (chociaż można argumentować, że byłeś narażony od momentu zainstalowania oprogramowania). Nowy personel dołączy do firmy i będzie potrzebował szkolenia w zakresie praktyk bezpieczeństwa i świadomości. Charakter samych zagrożeń zmienia się cały czas. Bezpieczeństwo to ciągły proces na wielu różnych poziomach. Chociaż testy penetracyjne są doskonałym uzupełnieniem tego procesu, nie są one celem samym w sobie ani szybkim rozwiązaniem. Jest to coś, co musi być przeprowadzane regularnie, aby mieć jakąkolwiek długoterminową wartość wewnętrzną, a nawet wtedy nie ma gwarancji, że powstrzyma to złoczyńców. Testowanie jest tak dobre, jak osoby je przeprowadzające.

Podstawowe bezpieczeństwo fizyczne

Kiedy mówimy o bezpieczeństwie fizycznym (lub ogólnie o bezpieczeństwie), kluczowym zwrotem, o którym należy pamiętać, jest „głęboka obrona". Twoim celem jest jak największe zminimalizowanie danego zagrożenia i podejście to powinno być wielowarstwowe.

Zacznij od rozważenia zasobów, które chcesz zabezpieczyć, a następnie przejdź na zewnątrz, myśląc o takich rzeczach, jak bezpieczeństwo pomieszczeń, bezpieczeństwo budynku i sama granica. To jest coś, co należy przemyśleć przed opracowaniem polityki bezpieczeństwa. W rzeczywistości powrócimy teraz do kilku obszarów omówionych wcześniej w rozdziale 10. Zwróć szczególną uwagę na następujące punkty:

• konsekwencje, które wynikałyby z kradzieży lub utraty majątku;

• poziom zagrożenia i wynikająca z niego podatność;

• wartość (finansową lub inną), ilość i charakter aktywów, które musisz chronić;

• wyjątkowe okoliczności w konkretnym miejscu, na przykład środowisko i lokalizacja oraz to, czy pomieszczenia są wspólne.

Obszary biurowe

W każdym środowisku biurowym, ale szczególnie w otwartym planie, należy wprowadzić „politykę czystego biurka”. Ma to na celu przede wszystkim zapewnienie, że poufne materiały nie zostaną pozostawione w pobliżu, ale należy je zastosować do wszystkich danych, na przykład karteczek samoprzylepnych i notatek. Monitory komputerów nie powinny być ustawione w sposób umożliwiający lub zachęcający do ukrytego monitorowania przez okna, powierzchnie odblaskowe lub podobne. Teoretycznie ekrany powinny być widoczne tylko dla użytkownika, a użytkownik powinien być świadomy, że jest obserwowany, chociaż nie zawsze jest to praktyczne w środowisku biurowym. Jeśli jest to opłacalne finansowo, używaj monitorów, które nie są widoczne, gdy są oglądane pod kątem; jest to właściwość niektórych marek płaskich ekranów.

Bezpieczeństwo budynku

Pożądane jest, aby mieć jak najmniej punktów wejścia i wyjścia, na ile jest to praktycznie i bezpiecznie możliwe. Tam, gdzie te punkty istnieją, upewnij się, że są odpowiednio objęte kontrolą dostępu, systemami wykrywania włamań i strażami. Żaden fizyczny mechanizm bezpieczeństwa nie jest nie do pokonania, ale Twoim celem powinny być trzy D: odstraszanie wtargnięcia, wykrywanie wtargnięcia i opóźnianie penetracji lub ucieczki intruza. Fizyczną kontrolę dostępu można zapewnić poprzez połączenie ludzkich strażników i różnych środków technicznych, które należy rozmieścić z myślą o maksymie „obrony w głębi”. Nie należy polegać na żadnym środku bezpieczeństwa. W szczególności zapewnienie bezpieczeństwa nie powinno polegać wyłącznie na personelu pierwszej linii, takim jak recepcjoniści. Powinny zostać uzupełnione o:

• system przepustek lub identyfikatorów;

• drzwi, kołowroty i tak dalej;

• losowe wyszukiwanie przy wejściach i wyjściach (w stosownych przypadkach i prawnie dopuszczalne);

• CCTV.

Ponieważ jednak pracownicy pierwszej linii są z natury narażeni na większe ryzyko, ich dobór należy starannie rozważyć.

Bezpieczeństwo obwodowe

Obwód może oznaczać wiele rzeczy. Można go zdefiniować za pomocą dowolnej kombinacji następujących elementów:

• naturalna granica;

• ogrodzenia lub ściany;

• bariery dla pojazdów, takie jak pachołki;

• zewnętrzna ściana samego budynku.

Z punktu widzenia bezpieczeństwa obwód tworzy granicę fizyczną, psychologiczną i prawną. Skuteczność granicy jako środka bezpieczeństwa jest zwiększona dzięki wdrożeniu różnych systemów wykrywania włamań na terenie, takich jak:

• patrole strażnicze;

• oświetlenie iluminacyjne bezpieczeństwa;

• CCTV.

Po raz kolejny hasłem przewodnim jest „głęboka obrona”. Oświetlenie iluminacyjne jest doskonałym środkiem, ponieważ zapewnia odstraszanie w nocy i natychmiast poprawia możliwości wykrywania intruzów, ale tylko wtedy, gdy istnieją patrole straży lub CCTV, aby wykorzystać lepszą widoczność zapewnianą przez oświetlenie.

Podsumowanie

Skupiliśmy się na atakującym, aby przyjrzeć się niektórym sposobom, w jakie możesz pomyśleć o ochronie przed atakami opisanymi w tej książce. Z tej perspektywy w rozsądnym stopniu pokrywa się z Częścią 10, w którym dyskusja dotyczyła formalnej dokumentacji polityki bezpieczeństwa. Obszary omówione w tym rozdziale obejmują:

• Zrozumienie źródeł ujawniania informacji - wiele wycieków informacji, na które narażona jest organizacja, jest nieumyślnych i przypadkowych, chociaż wiele z nich tak nie jest. Wiedza o swoich słabych stronach i łagodzenie tych obszarów ma kluczowe znaczenie. Podane przykłady obejmują ograniczanie informacji na firmowych stronach internetowych i edukowanie personelu w zakresie ograniczania informacji, które można wykorzystać, które publikują na swój temat w Internecie.

• Łagodzenie zagrożenia atakami socjotechnicznymi - Zrozumienie zagrożenia i edukacja personelu to podstawa. Personel powinien zdawać sobie sprawę z wartości nawet pozornie nieszkodliwych informacji w rękach napastnika i umieć rozpoznać potencjalne ataki socjotechniczne. • Zmniejszanie ryzyka elektronicznego monitorowania - istnieje wiele sposobów wykrycia tego problemu (znanego również jako podsłuch).

• Zaangażowanie zespołu ds. Testów penetracyjnych - testy penetracyjne, zarówno fizyczne, jak i elektroniczne, są wysoce zalecane, aby uzyskać wgląd w aktualny stan bezpieczeństwa. Ostrzegamy jednak, że zespoły testujące nie mają równego doświadczenia ani kompetencji.

• Bezpieczeństwo podstawowe - są to rzeczy, które naprawdę musisz ograniczyć, zanim skoncentrujesz się na bardziej złożonych aspektach bezpieczeństwa fizycznego lub systemu.