Fizyczne bezpieczeństwo jest prawdopodobnie najbardziej krytycznym obszarem bezpieczeństwa IT, aby zapobiec utracie lub kradzieży poufnych danych. Jeśli organizacja nie zdoła wyegzekwować odpowiedniego zabezpieczenia fizycznego, wszelkie inne techniczne środki bezpieczeństwa, takie jak zapory ogniowe i systemy wykrywania włamań (IDS), mogą zostać ominięte. Jest takie powiedzenie: "Kiedy jesteś w środku, jesteś właścicielem sieci." Zabezpieczając fizycznie swoją sieć i organizację, uniemożliwiasz komuś kradzież sprzętu, takiego jak laptopy lub napędy taśmowe, umieszczanie keyloggerów sprzętowych w systemach i zasadzanie nieautentycznego dostępu punkty w sieci. Fizyczne bezpieczeństwo zależy w dużej mierze od jednostek, aby go egzekwować i dlatego jest podatne na ataki socjotechniczne, takie jak podążanie za pracownikiem do budynku bez dostarczania odpowiedniego klucza lub poświadczeń (przez to obejście problemu bezpieczeństwa fizycznego). W tym rozdziale zbadamy potrzebę bezpieczeństwa fizycznego i określimy, kto jest odpowiedzialny za planowanie i egzekwowanie tego bezpieczeństwa.

Komponenty bezpieczeństwa fizycznego

Fizyczne bezpieczeństwo to ochrona personelu, sprzętu, programów, sieci i danych pochodzących z fizycznych okoliczności i zdarzeń, które mogą spowodować poważne straty lub szkody dla przedsiębiorstwa, agencji lub instytucji. Obejmuje to ochronę przed ogniem, klęskami żywiołowymi, włamaniem, kradzieżą, aktami wandalizmu i terroryzmem. Fizyczne bezpieczeństwo jest często pomijane (a jego znaczenie niedoszacowane) na rzecz bardziej technicznych i dramatycznych problemów, takich jak włamania, wirusy, trojany i spyware. Jednak naruszenia bezpieczeństwa fizycznego mogą być dokonywane przy niewielkiej lub żadnej wiedzy technicznej na temat atakującego. Ponadto wypadki i klęski żywiołowe są częścią codziennego życia, a na dłuższą metę są nieuniknione. Istnieją trzy główne elementy bezpieczeństwa fizycznego:

* Przeszkody mogą stanowić przeszkodę dla potencjalnych intruzów, a strony mogą zostać utwardzone aby zapobiegać wypadkom i katastrofom ekologicznym. Takie środki mogą obejmować wiele zamków, ogrodzeń, ścian, ognioodpornych sejfów i tryskaczy.

* Można wprowadzić systemy nadzoru i powiadamiania, takie jak oświetlenie, czujniki ciepła, czujniki dymu, czujki włamaniowe, alarmy i kamery.

* Metody można zaimplementować w celu zatrzymania napastników (najlepiej przed zniszczeniem) i szybkiego powrotu do zdrowia po wypadkach, pożarach lub klęskach żywiołowych.

Wydaje się, że każdego dnia artykuły prasowe opisują inną znaną agencję rządową lub poważną korporację, która naruszyła informacje o klientach lub poufne informacje o pracownikach. Na przykład laptop może zostać skradziony podczas napadu na inwazję w domu lub z pokoju hotelowego, podczas gdy pracownik podróżuje. Ta poufna lub poufna informacja może być niebezpieczna w rękach hakera. W fizycznym bezpieczeństwie, podobnie jak w przypadku wszystkich zabezpieczeń, najlepszym podejściem jest warstwowa obrona. Nigdy nie powinieneś polegać w 100% na jednej kontroli, aby chronić swoje krytyczne aktywa. Oto dwa przykłady tego, gdzie warstwowe podejście do bezpieczeństwa fizycznego jest lepsze niż jeden mechanizm fizycznego bezpieczeństwa. Pierwszy przykład to sytuacja, w której strażnik jest jedynym mechanizmem obronnym. Jeśli zasypia lub podejmuje niezaplanowaną przerwę, intruz ma możliwość wejścia do centrum danych bez wykrycia. Lepszym środkiem bezpieczeństwa byłoby posiadanie osoby wymagającej posiadania unikalnego identyfikatora, aby wejść do drzwi wejściowych. Następnie rzuca wyzwanie strażnikowi, nagranemu w kamerze, a następnie musi mieć oddzielny unikalny klucz do wejścia do centrum danych. W tym przykładzie istnieją cztery warstwy obrony, które chronią Twoje zasoby. W drugim przykładzie bezpieczeństwa pracownik nie może sobie pozwolić na laptopa, więc postanawia zabrać ze sobą komputer dla swojej ulubionej gry wideo. W drodze do domu rozprasza go pociąg lub autobus i

zapomina o torbie z laptopem. Laptop nie ma żadnych mechanizmów kontroli bezpieczeństwa i zawiera poufne dane. Jeśli w tym scenariuszu zastosowano najlepsze praktyki, istniałoby wiele warstw, aby zapobiec i zniechęcić tę osobę do usunięcia laptopa z kontrolowanego środowiska. Należy wprowadzić zasady dopuszczalnego użytkowania, aby podkreślić znaczenie i konsekwencje usunięcia własności korporacyjnej i danych wrażliwych z lokalu. Laptop powinien mieć włączone uwierzytelnianie wieloczynnikowe i szyfrowanie dysku, tak aby w przypadku jego zgubienia lub kradzieży dane na nim zawarte były bezużyteczne dla innych. Jeśli środowisko było szczególnie wrażliwe, urządzenia śledzące mogły być umieszczone na wszystkich urządzeniach mobilnych, a w przypadku, gdy podróżują one niedopuszczalnie daleko od biura, uruchamiany jest alarm powiadamiający personel ochrony. Bardzo ważne jest, aby mieć wiele linii obrony, ponieważ im więcej warstw obrony masz, tym mniej jesteś podatny na zagrożenie. Ważne jest również, aby pamiętać, że możesz mieć wiele warstw logicznych zabezpieczeń, które chronią zasoby i można je łatwo ominąć szybko i łatwo, jeśli uzyska się fizyczny dostęp. Kradzież sprzętu jest jednym z najczęstszych ataków fizycznych. Większość ludzi nie spodziewa się, że ich komputer zostanie skradziony i będzie naiwny w kwestii blokowania systemów hosta; zamiast tego polegają na standardowych mechanizmach bezpieczeństwa sieci. Wiele ataków wewnętrznych jest wynikiem fizycznych naruszeń bezpieczeństwa. Gdy haker uzyska fizyczny dostęp do serwera, pojedynczego systemu klienckiego lub portu sieciowego, wyniki mogą być katastrofalne. Ponadto takie naruszenia są trudne do zidentyfikowania, śledzenia lub zlokalizowania. Niektóre typowe naruszenia bezpieczeństwa spowodowane niewystarczającym bezpieczeństwem fizycznym są następujące:

* Instalacja szkodliwego oprogramowania, takiego jak keyloggery, wirusy, trojany, backdoory lub rootkity

* Identyfikacja i przechwytywanie danych uwierzytelniających lub uwierzytelniających, takich jak hasła lub certyfikaty

* Fizyczne połączenie z siecią przewodową w celu wykrywania poufnych danych, takich jak hasła i numery kart kredytowych

* Dostęp do systemów w celu zbierania danych, których można użyć do złamania NN-owego hasła przydzielonego lokalnie w systemie

* Możliwość umieszczenia nieuczciwych punktów dostępu w celu utworzenia otwartej sieci bezprzewodowej za pomocą dostępu do sieci przewodowej

* Kradzież dokumentów papierowych lub elektronicznych

* Kradzież poufnych informacji faksu

* Atak nurkowy Dumpster (podkreślający konieczność niszczenia ważnych dokumentów)

Wskazania fizyczne naruszenia bezpieczeństwa mogą obejmować, ale nie są ograniczone do

* Nieautoryzowane lub niewyjaśnione alarmy drzwi

* Nieautoryzowany personel nagrany kamerą bezpieczeństwa

* Uszkodzenie zamka drzwi lub zewnętrznego ogrodzenia bariery

* Dowód na pojazdy lub osoby znajdujące się na zewnątrz i wewnątrz ogrodzenia

* Utrata komunikacji, której nie można wyjaśnić

* Brakujące lub nieokreślone dla wyposażenia

Zrozumienie bezpieczeństwa fizycznego

Ogólnie środki bezpieczeństwa można podzielić na trzy następujące sposoby:

Fizyczne .Fizyczne środki zapobiegające dostępowi do systemów obejmują ochronę, oświetlenie, ogrodzenia, blokady i alarmy. Punkty dostępu do obiektów powinny być ograniczone i powinny być monitorowane / chronione przez kamery i alarmy z kamerami przemysłowymi (CCTV). Wejście do obiektu powinno być ograniczone do osób upoważnionych. Dostęp do systemów przenośnych i nośników wymiennych, takich jak dyski wymienne, taśmy kopii zapasowych i dyski, powinien być ograniczony i zabezpieczony. Ekrany komputerowe powinny być ustawione w taki sposób, aby nie były widoczne dla przechodniów, a polityka powinna być wdrożona i egzekwowana, co wymaga od użytkowników blokowania systemów, gdy opuszczają komputer z dowolnego powodu. Systemy komputerowe z bardzo wrażliwymi danymi powinny być chronione w zamkniętym i zablokowanym obszarze, takim jak pomieszczenie dostępu do poświadczeń z walizką do montażu w stojaku i zamkiem.

Techniczne środki bezpieczeństwa .Techniczne, takie jak zapory ogniowe, IDS, filtrowanie treści spyware oraz skanowanie wirusów i trojanów powinny być wdrażane we wszystkich zdalnych systemach klienckich, sieciach i serwerach. Techniczne środki bezpieczeństwa, takie jak kontrola dostępu, są realizowane za pomocą uwierzytelniania, haseł oraz uprawnień do plików i folderów. Inne kontrole techniczne można wdrożyć za pomocą oprogramowania komputerowego, takiego jak skanowanie wirusów i zapory hosta. Zasadniczo kontrola techniczna to dowolny mechanizm bezpieczeństwa zaimplementowany za pomocą sprzętu komputerowego lub oprogramowania.

Operacyjne Bezpieczeństwo operacyjne jest rozwiązywane za pomocą mechanizmów kontrolnych, takich jak akceptowalne zasady użytkowania, zasady zatrudniania i zasady bezpieczeństwa. Operacyjne środki bezpieczeństwa służące analizie zagrożeń i przeprowadzaniu ocen ryzyka powinny być udokumentowanym procesem w polityce bezpieczeństwa organizacji. Potrzebujesz środków bezpieczeństwa fizycznego z tego samego powodu, dla którego potrzebujesz innych rodzajów zabezpieczeń (takich jak techniczne lub operacyjne): aby uniemożliwić hakerom uzyskanie dostępu do twojej sieci i twoich informacji. Haker może łatwo uzyskać taki dostęp poprzez słabości fizyczne

Środki bezpieczeństwa. Ponadto dane mogą zostać utracone lub uszkodzone z przyczyn naturalnych, więc menedżerowie ds. Ryzyka muszą uwzględnić klęski żywiołowe w równaniu przy planowaniu odpowiednich zabezpieczeń. Środki bezpieczeństwa fizycznego mają na celu zapobiegać:

* Nieautoryzowany dostęp do systemu komputerowego

* Kradzież danych z systemów

* Korupcja danych przechowywanych w systemie

* Utrata danych lub uszkodzenie systemów spowodowane przyczynami naturalnymi

Dane skradzione z laptopa VA

W 2006 r. Skradziono laptopa z domu analityka Departamentu Spraw Weteranów, który (wbrew polityce departamentu) zabrał komputer do domu. Laptop zawierał dane o około 26,5 miliona amerykańskich weteranów wojskowych. Uważa się, że było to przypadkowe włamanie, a osoba, która ukradła laptopa, nie wiedziała, że dane znajdują się na komputerze. Złodzieje zabrali zarówno swój laptop, jak i zewnętrzny dysk twardy zawierający nazwiska, daty urodzenia i numery ubezpieczenia społecznego każdego weterana, który został zwolniony po 1975 roku. VA zauważyła, że pracownik

"zabrał do domu znaczną ilość danych elektronicznych z VA, które nie był do tego upoważniony. Było to z naruszeniem naszych zasad, przepisów i zasad. "To naruszenie bezpieczeństwa jest przykładem tego, jak twoje najbardziej osobiste dane mogą łatwo dostać się w ręce złodziei tożsamości. Kilka grup weteranów podjęło kroki prawne przeciwko VA po ujawnieniu naruszenia. Trzy lata później, strony osiągnęły porozumienie. Weterani, którzy mogą udowodnić faktyczne szkody, takie jak emocjonalny stres prowadzący do fizycznych symptomów lub wydatki na monitorowanie kredytu, będą uprawnieni do otrzymywania płatności do wysokości 1500 USD. Rozliczenie to wynosi 20 milionów USD kosztów poniesionych przez VA. Jest to tylko jeden przykład tego, jak ważne jest fizyczne bezpieczeństwo stron i egzekwowanie zasad w celu utrzymania bezpieczeństwa danych osobowych. Organizacje uznane za odpowiedzialne za brak ochrony danych, którym zostały powierzone, mogą zostać obciążone wysokimi grzywnami.

Następujące osoby w organizacji powinny ponosić odpowiedzialność za bezpieczeństwo fizyczne:

* Oficer ochrony fizycznej organizacji

* Specjaliści systemów informacyjnych

* Główny specjalista informatyczny

* Pracownicy

Zasadniczo każdy w organizacji jest odpowiedzialny za egzekwowanie zasad bezpieczeństwa fizycznego . Zadaniem fizycznego pracownika ochrony jest ustalenie standardu bezpieczeństwa fizycznego i wdrożenie środków bezpieczeństwa fizycznego. Organizacje ponoszą odpowiedzialność za przeszkolenie wszystkich pracowników w zakresie szkoleń dotyczących bezpieczeństwa. Najlepszym środkiem zapobiegającym atakom na bezpieczeństwo fizyczne jest szkolenie pracowników świadomych naruszenia bezpieczeństwa fizycznego. Na bezpieczeństwo fizyczne wpływają czynniki niezależne od fizycznych zabezpieczeń. Czynniki, które mogą wpływać na fizyczne bezpieczeństwo organizacji, obejmują:

* Wandalizm

* Kradzież

* Przyczyny naturalne, takie jak trzęsienie ziemi, pożar lub powódź

Specjaliści ds. Bezpieczeństwa muszą być świadomi tych czynników ryzyka i odpowiednio planować. Wiele organizacji tworzy plan ciągłości działania (BCP) lub plan przywracania po awarii (DRP), aby przygotować się na te możliwości.

Fizyczne zabezpieczenia strony

Istnieje kilka prostych sposobów na poprawę bezpieczeństwa fizycznego w organizacji. Wielokrotne poprawianie bezpieczeństwa wymaga egzekwowania wytycznych, które już istnieją. Ludzie po pewnym czasie tracą swobodę w egzekwowaniu zasad i procedur. Aby utrzymać wysoki poziom bezpieczeństwa, wszyscy członkowie organizacji muszą zachować czujność w zakresie ochrony danych zgody organizacji. Aby zapewnić silne fizyczne bezpieczeństwo witryny, należy wdrożyć następujące środki zaradcze:

Zablokuj serwerownię. Zanim zablokujesz serwery za pomocą mechanizmów technicznych i zanim włączysz je po raz pierwszy, powinieneś upewnić się, że na drzwiach do serwerowni są dobre blokady. Oczywiście najlepsza kłódka na świecie nie działa dobrze, jeśli nie jest używana, więc potrzebujesz również zasad, które wymagałyby, aby drzwi były zamknięte za każdym razem, gdy pokój nie jest zajęty. Zasady powinny określać, kto ma klucz lub kod dostępu. Serwerownia jest sercem sieci fizycznej, a ktoś

mający fizyczny dostęp do serwerów, przełączników, routerów, kabli i innych urządzeń w tym pomieszczeniu może zrobić ogromne uszkodzić.

Skonfiguruj i monitoruj nadzór wideo. Zablokowanie drzwi do serwerowni to dobry pierwszy krok, ale ktoś może się włamać lub ktoś, kto ma autoryzację dostępu, może niewłaściwie użyć tego organu. Potrzebujesz sposobu, by dowiedzieć się, kto wchodzi i wychodzi oraz kiedy. Dziennik do logowania i wylogowywania to najbardziej elementarny sposób na osiągnięcie tego celu, ale to podejście ma wiele wad. Osoba o złych zamiarach może ją po prostu ominąć. Lepszym rozwiązaniem niż dziennik pokładowy jest system uwierzytelniania wbudowany w urządzenia blokujące, dlatego do odblokowania drzwi wymagana jest karta inteligentna, token lub skanowanie biometryczne, a także zapis tożsamości każdego wprowadzającego. Kamera nadzoru wideo, umieszczona w miejscu utrudniającym manipulowanie lub wyłączanie, ale zapewniająca dobry widok osób wchodzących i wychodzących, powinna uzupełniać dziennik pokładowy lub elektroniczny system dostępu. Kamery nadzoru mogą monitorować w sposób ciągły lub mogą wykorzystywać technologię wykrywania ruchu do nagrywania tylko wtedy, gdy ktoś się porusza. Mogą nawet zostać skonfigurowane do wysyłania powiadomień e-mailem lub telefonem komórkowym, jeśli ruch zostanie wykryty, gdy nie będzie, np. Po godzinach.

Upewnij się, że najbardziej wrażliwe urządzenia znajdują się w zamkniętym pomieszczeniu. To nie tylko serwery że musisz fizycznie zabezpieczyć. Trzeba też zabezpieczyć inny sprzęt sieciowy. Haker może podłączyć laptopa do koncentratora i użyć oprogramowania sniffer do przechwytywania danych podróżujących przez sieć. Upewnij się, że jak najwięcej twoich urządzeń sieciowych jest w tym zamkniętym pomieszczeniu. Szafy elektryczne i pokoje telefoniczne są łatwymi celami, jeśli nie są zabezpieczone.

Zabezpiecz stacje robocze. Hakerzy mogą używać dowolnego niezabezpieczonego komputera podłączonego do sieci, aby uzyskać dostęp do lub usunąć informacje, które są ważne dla Twojej firmy. Stacje robocze w pustych biurkach lub w pustych biurach - takie jak te używane przez pracowników, którzy są na wakacjach lub którzy opuścili firmę i nie zostali jeszcze zastąpieni - lub w miejscach łatwo dostępnych dla osób postronnych - takich jak recepcja recepcji - są szczególnie narażone. Odłącz i / lub usuń komputery, które nie są używane i / lub blokuj drzwi pustych biur, w tym te, które są tymczasowo puste, gdy pracownik jest na lunchu lub choruje. W przypadku komputerów, które muszą pozostać w otwartych przestrzeniach, czasem poza zasięgiem pracowników, należy włączyć czytniki kart inteligentnych lub biometrycznych, aby trudniej było nieuprawnionym osobom zalogować się.

Zachowaj intruzów przed otwarciem komputera. Zarówno serwery, jak i stacje robocze powinny być chronione przed złodziejami, którzy mogą otworzyć skrzynkę i pobrać dysk twardy. O wiele łatwiej jest wynieść z dysku twardego w kieszeni niż nosić pełną wieżę z lokalu. Wiele komputerów wyposażonych jest w zamki do etui, które uniemożliwiają otwarcie obudowy bez klucza.

Chroń przenośne urządzenia. Laptopy i komputery przenośne stanowią szczególne zagrożenie dla bezpieczeństwa fizycznego. Złodziej może łatwo ukraść cały komputer, w tym wszelkie dane przechowywane na jego dysku, a także hasła logowania do sieci, które mogą zostać zapisane. Jeśli pracownicy używają laptopów przy biurkach, powinni zabrać je ze sobą, gdy opuszczą lub zabezpieczyć je na stałe urządzenie z blokadą. Urządzenia podręczne można zamknąć w szufladzie bezpiecznie, gdy pracownik opuszcza teren. Alarmy wykrywające ruch są również dostępne, aby ostrzec Cię, jeśli twój przenośny jest przenoszony. W przypadku urządzeń przenośnych, które zawierają poufne informacje, pełne szyfrowanie dysku, czytniki biometryczne i oprogramowanie, które "dzwoni do domu", jeśli skradziony laptop łączy się z Internetem, mogą uzupełniać fizyczne środki ostrożności.

Wiele smartfonów ma możliwość zdalnego czyszczenia, jeśli urządzenie zostanie zgubione lub skradzione.

Spakuj kopie zapasowe. Tworzenie kopii zapasowych ważnych danych jest podstawowym elementem odzyskiwania po awarii, ale nie zapominaj, że informacje o tych kopiach zapasowych, dyskach lub dyskach mogą zostać skradzione i wykorzystane przez kogoś spoza firmy. Wielu administratorów IT utrzymuje kopie zapasowe obok serwera w serwerowni. Powinny być zamknięte w szufladzie lub przynajmniej bezpieczne. W idealnej sytuacji zbiór kopii zapasowych powinien być przechowywany poza terenem zakładu, a użytkownik musi zadbać o to, aby był on zabezpieczony w tej lokalizacji poza siedzibą. Nie zapomnij o tym, że niektórzy pracownicy mogą tworzyć kopie zapasowe swoich prac na dyskietkach, kluczach USB lub zewnętrznych dyskach twardych. Jeśli ta praktyka jest dozwolona lub zachęcana, upewnij się, że masz zasady wymagające, aby kopie zapasowe były zawsze zamknięte.

Wyłącz napędy dysków wymiennych. Aby uniemożliwić pracownikom kopiowanie informacji firmowych na nośniki wymienne, można wyłączyć lub usunąć stacje dysków, porty USB i inne sposoby podłączania dysków zewnętrznych. Proste odłączenie kabli może nie zniechęcić technicznie doświadczonych pracowników. Niektóre organizacje posuwają się tak daleko, aby wypełnić porty klejem lub innymi substancjami, aby na stałe uniemożliwić ich użycie, chociaż istnieją mechanizmy programowe, które uniemożliwiają to i pozwalają administratorowi na ponowne włączenie napędu.

Chroń swoje drukarki. Być może nie myślisz o drukarkach stwarzających zagrożenie dla bezpieczeństwa, ale wiele dzisiejszych drukarek zapisuje zawartość dokumentów we własnych pamięciach podręcznych. Jeśli haker kradnie drukarkę i uzyskuje dostęp do tej pamięci, może on wykonywać kopie ostatnio drukowanych dokumentów. Drukarki, takie jak serwery i stacje robocze przechowujące ważne informacje, powinny znajdować się w bezpiecznych lokalizacjach i przykręcane, aby nikt nie mógł z nich wyjść. Pomyśl także o fizycznym bezpieczeństwie dokumentów drukowanych przez pracowników. Najlepiej wdrożyć politykę natychmiastowego niszczenia niechcianych wydrukowanych dokumentów, nawet tych, które nie zawierają poufnych informacji. Ustanawia to nawyk i uwalnia użytkownika końcowego od odpowiedzialności za określenie, czy dokument powinien zostać rozdrobniony.

Wymuszaj dyskietki dla wszystkich pracowników i kontrahentów. Zainicjuj program znaczków, który zawiera zdjęcie pracownika oraz obszary dostępu oznaczone kolorami. Wykonawcy i odwiedzający powinni również posiadać odznaki i być eskortowani, obserwowani i nadzorowani przez całą swoją wizytę. Standardowa zasada obowiązująca wszystkich pracowników powinna dotyczyć każdego, kto nie ma widocznego identyfikatora.

Uważaj na „tailgatersów”. Ci ludzie czekają na kogoś z dostępem, aby wejść do kontrolowanego obszaru, takiego jak ten z zamkniętymi drzwiami, a następnie podążać za upoważnioną osobą przez drzwi. Tailogaters wchodzą bez własnego klucza, klucza karty lub kombinacji zamków. Palacze, którzy stoją na zewnątrz budynku, wydają się szczególnie podatni na "tailgating"; po podzieleniu się czasem i dymkiem wspólnie, normalne jest trzymanie drzwi otwartych dla innych palaczy po zakończeniu przerwy na dymek. Nie wszystkie ataki na dane organizacji występują w sieci, a nie wszystkie ataki mają charakter techniczny. Konieczne jest, aby firmy pamiętały, że utrzymywanie silnego programu bezpieczeństwa sieci nie chroni ich przed fizycznym atakiem lub kradzieżą danych oraz zasobami, które zawierają te dane. Fizyczne ataki mogą pochodzić spoza organizacji, ale mogą również być osobami wewnętrznymi - powszechnie uważa się, że niezadowoleni pracownicy lub kontrahenci są źródłem fizycznych ataków na witryny. Zobacz ćwiczenie 11.2.

Ćwiczenie 11. 2

Dokonaj inspekcji fizycznego bezpieczeństwa witryny swojej organizacji. Przejrzyj poniższą listę kontrolną zabezpieczeń fizycznej witryny, aby ocenić fizyczne bezpieczeństwo organizacji.

Publiczne parkingi

* W razie potrzeby, wyraźnie wskazano obszary parkingowe dla pracowników, najemców i parkingów publicznych?

* Czy poziom oświetlenia w nocy jest wystarczający? Test: Czy możesz wygodnie czytać gazetę w istniejących warunkach oświetleniowych?

* Czy parkingi i wejścia są widoczne dla jak największej liczby osób?

* Czy miejsca parkingowe są w pełni oświetlone przez wszystkie godziny przebywania osób na terenie posesji?

* W razie potrzeby, czy miejsca parkingowe zostały prawidłowo oddane do użytku? Czy nie zezwala się organom ścigania na podjęcie działań egzekucyjnych w razie potrzeby? Przykłady: ograniczone parkingi, parking dla osób niepełnosprawnych.

Ograniczone obszary dostępu

* Czy są zainstalowane bariery, takie jak ogrodzenia i zamknięte bramy, aby uniemożliwić nieupoważnionemu dostępowi do pojazdów i pieszych dostęp do obszarów o ograniczonym dostępie?

* Czy pracownicy są poinstruowani, aby zgłaszać nieupoważnione osoby w obszarach o ograniczonym dostępie oraz innych podejrzanych osób i działań?

* Czy obszary objęte ograniczeniami są prawidłowo publikowane, aby zapobiec nieupoważnionym osobom?

* Czy oznakowanie na zewnątrz jest wyraźnie widoczne w pobliżu obszarów o ograniczonym dostępie?

* Czy oznakowanie wskazuje numer telefonu do zgłaszania podejrzanej aktywności w łatwo widocznym miejscu?

Powierzchnie magazynowe

* Czy miejsca i powierzchnie magazynowe są całkowicie zamknięte?

* Czy ogrodzenia i ściany są dobrze naprawione?

* Czy ogrodzenia są wystarczająco wysokie?

* Czy bramy są w dobrym stanie technicznym?

* Czy powierzchnie magazynowe i place są wyposażone w odpowiednie oświetlenie w godzinach ciemności?

* Czy bramy są zabezpieczone za pomocą kłódek o wysokim poziomie bezpieczeństwa lub równoważnych urządzeń blokujących?

* Czy kłódki są zablokowane, gdy otwierają się bramy?

* Czy obszary pamięci o wysokiej wartości są chronione przez elektroniczny system bezpieczeństwa?

Budynek z zewnątrz

* Czy wejścia publiczne są jasno zdefiniowane przez chodniki i oznakowanie?

* Czy funkcje krajobrazu są utrzymywane, aby zapewnić dobrą widoczność wokół budynków? Czy roślinność przycięta została w celu wyeliminowania potencjalnych kryjówek w pobliżu drzwi, okien, chodników i innych wrażliwych obszarów nieruchomości?

* Czy drzewa lub inne elementy krajobrazu zapewniają dostęp do dachu lub innych wyższych poziomów budynków?

* Czy drzewa i roślinność są przycięte, aby nie zakłócały oświetlenia i widoczności?

* Czy pojemniki na śmieci i pojemniki na śmieci tworzą plamki lub kryjówki?

* Czy ogrodzenia obwodowe są zaprojektowane tak, aby zachować widoczność z ulicy?

* Czy zewnętrzne obszary prywatne są łatwe do odróżnienia od obszarów publicznych?

Oświetlenie

* Budujemy powierzchnie zewnętrzne i inne krytyczne obszary oświetlone zgodnie z zalecanymi poziomami w godzinach ciemności?

* Czy we wszystkich otworach drzwi i okien oraz innych wrażliwych punktach utrzymują się właściwe poziomy oświetlenia w godzinach ciemności?

* Czy został ustanowiony harmonogram przeglądów konserwacyjnych, aby zapewnić, że światła są w dobrym stanie przez cały czas?

Drzwi

* Czy wszystkie drzwi zewnętrzne wykonane są z metalu, metalu i szkła lub z litego drewna?

* Czy wszystkie nieużywane drzwi są na stałe zamknięte?

* Czy zewnętrzny sprzęt został usunięty ze wszystkich drzwi, które nie są używane do zapewnienia dostępu z zewnątrz?

* Czy wszystkie drzwi są zaprojektowane w taki sposób, że nie można uzyskać zwolnienia blokady przez wyłamywanie szyb lub lekkich paneli?

* Czy przesuwne szklane drzwi są wyposażone w dodatkowe zamki pinowe i urządzenia zapobiegające podnoszeniu?

* Czy odkryte zawiasy mają nieusuwalne styki?

* Czy zamki z zasuwą o dobrej jakości są stosowane, gdy tylko jest to możliwe?

* Czy zaprojektowano zamek lub konstruowano ościeżnicę tak, aby drzwi nie mogły zostać otwarte przez rozłożenie ramy?

* Czy klucze są wydawane tylko osobom, które faktycznie ich potrzebują?

* Czy obowiązują zasady nakazujące, aby wszystkie drzwi, które nie muszą być odblokowane w godzinach pracy, były zamknięte i zabezpieczone, gdy nie są używane?

Okna

* Czy nieużywane okna są na stałe zamknięte?

* Czy zamki okienne są zaprojektowane lub umiejscowione tak, aby nie mogły zostać pokonane przez rozbicie szkła?

* Gdzie to stosowne, czy występują elementy krajobrazu, takie jak cierniste krzewy lub podobna roślinność, stosowane w celu uniemożliwienia dostępu do wrażliwych okien?

* Gdzie to konieczne, czy dostępne okna są odpowiednio oświetlone, czy nie ma godzin ciemności?

* Czy drabiny dachowe i inne punkty dostępu do dachów zostały usunięte lub zabezpieczone przed nieautoryzowanym użyciem?

* Czy drzwi zwijane i przesuwne są prawidłowo zamontowane i zabezpieczone za pomocą wysokiej jakości urządzeń blokujących?

* Czy pomieszczenia gospodarcze zarówno wewnątrz, jak i na zewnątrz budynku są odpowiednio zabezpieczone?

Publiczne obszary dostępu

*Czy obszary bezpieczeństwa i / lub recepcji są ustawione tak, aby wyświetlać wszystkie publiczne wejścia?

* Czy wszystkie pomieszczenia ogólnodostępne w budynku są wyraźnie oznaczone?

* Czy granice między obszarami publicznymi i niepublicznymi są jasno określone?

* Czy zainstalowano bezpieczne bariery, aby zapobiec łatwemu przemieszczaniu się między obszarami publicznymi i niepublicznymi?

* Czy wszystkie drzwi prowadzą do prywatnych biur i innych obszarów niepublicznych zabezpieczonych przez wysokiej jakości urządzenia blokujące, takie jak zamki elektroniczne lub klawiatury?

*Czy pracownicy ochrony zatrudnieni są w obszarach, w których istnieje duże prawdopodobieństwo działalności przestępczej lub wkroczenia na teren ochrony?

* Czy wewnętrzne toalety publiczne są widoczne z pobliskich biur lub recepcji?

Bezpieczeństwo biur

* Czy ograniczasz klucze biurowe do tych, którzy ich potrzebują?

* Czy przechowujesz kompletne i aktualne dane dotyczące dyspozycji wszystkich kluczy biurowych?

* Czy posiadasz odpowiednie procedury zbierania kluczy od zerwanych pracowników?

* Czy zabezpieczasz wszystkie maszyny do pisania, kalkulatory, komputery i podobne przedmioty za pomocą jakiegoś urządzenia blokującego?

*Czy zabraniasz duplikowania kluczy biurowych z wyjątkiem tych, które są specyficzne zarządzone przez ciebie na piśmie?

* Czy wszystkie klucze biurowe muszą być oznaczone jako "Nie duplikuj", aby zapobiec wykonywaniu kopii przez legalnych ślusarzy bez Twojej wiedzy?

* Czy ustaliłeś zasady, że klucze nie będą pozostawione niestrzeżone na biurkach lub w szafkach - i czy egzekwujesz zasady?

* Nie będą oznaczone informacją identyfikującą obiekt, do którego należą?

* Czy chcesz, aby klucze szafki na dokumenty były usuwane z zamków i umieszczane w bezpiecznym miejscu, gdy nie są używane?

* Czy masz odpowiedzialną osobę odpowiedzialną za program kontroli kluczy?

* Czy niszczysz wrażliwe dokumenty przed ich odrzuceniem?

* Czy wieszasz teczki i torby zawierające ważne materiały w bezpiecznym miejscu, gdy nie są używane?

* Czy nalegasz na odpowiednią identyfikację od wszystkich dostawców i naprawę osób, które przychodzą do twojego zakładu?

* Czy co wieczór kasujecie ważne gazety?

* Czy często zmieniasz kombinację na swój sejf?

* Czy dostęp do komputera jest ograniczony do upoważnionego personelu?

* Czy wprowadziłeś system identyfikacyjny pracownika?

* Jeśli zatrudniasz strażników po godzinach, regularnie przeprowadzasz niezapowiedziane wizyty aby upewnić się, że wykonują oni swoją pracę właściwie?

Alarmy

* Czy twoje budynki są wyposażone w system alarmowy?

* Czy system alarmowy jest certyfikowany przez Underwriters Laboratory?

* Czy system jest testowany codziennie?

* Czy system zgłasza się do centralnej stacji alarmowej lub obiektu policji?

* Czy system ma automatyczny zapasowy zasilacz, który aktywuje się podczas awarii zasilania?

* Czy system jest wolny od fałszywych alarmów?

* Czy system wykorzystuje technologię antysabotażową?

Co robić po wystąpieniu naruszenia bezpieczeństwa

Nawet jeśli organizacja zastosuje fizyczne środki zaradcze w miejscu, naruszenie bezpieczeństwa może nadal występować. Jeśli dojdzie do takiego naruszenia, zalecane są pewne kroki, które organizacja powinna podjąć, aby zapobiec ponownemu wystąpieniu:

* Stwórz fizyczny proces reagowania na incydenty związane z bezpieczeństwem, w tym i NN uzgadnianie zagrożenia, odpowiedzi, odzyskiwania i przeglądu po incydencie w celu zarządzania atakiem fizycznym lub incydentem bezpieczeństwa.

* Ustaw zasady, standardy i procedury w celu obsługi zdarzenia związanego z bezpieczeństwem fizycznym, procesu odpowiedzi.

* Wskaż interesariuszy - w tym zespół reagowania na incydenty bezpieczeństwa, personel w organizacji i strony zewnętrzne, które prawdopodobnie będą zaangażowane w zarządzanie incydentem związanym z bezpieczeństwem informacji i przegląd.

Podsumowanie

Pamiętaj, że bezpieczeństwo sieci zaczyna się na poziomie fizycznym. Wszystkie zapory na świecie nie powstrzymają intruza, który jest w stanie uzyskać fizyczny dostęp do sieci i komputerów, więc zamknij się i zablokuj. Fizyczny dostęp do danych firmowych przez nieupoważnioną osobę stanowi atak na bezpieczeństwo organizacji. Gdy ktoś uzyska fizyczny dostęp do twoich danych - bez względu na to, czy jest to skradziony laptop, czy zgubione dokumenty lub nośniki - stajesz się podatny na kolejne ataki, nie wspominając już o złym rozgłosie. Istotne jest wdrożenie fizycznych środków bezpieczeństwa na stronie, aby zapobiec atakom, zanim one wystąpią.

Do Zapamiętania !

* Zapoznałeś się z atakami, które można wykonać poprzez fizyczny dostęp. Fizyczny dostęp daje hakerowi zdolność do łamania haseł, instalowania nieuczciwych punktów dostępu bezprzewodowego i kradzieży sprzętu.

* Poznałeś niektóre czynniki, które wpływają na egzekwowanie bezpieczeństwa fizycznego. Wandalizm, kradzież i przyczyny naturalne wpływają na egzekwowanie bezpieczeństwa fizycznego.

* Dowiedziałeś się, kto jest odpowiedzialny za bezpieczeństwo fizyczne. Oficer ochrony organizacji, specjaliści systemów informatycznych, główny informator i pracownicy są odpowiedzialni za bezpieczeństwo fizyczne.

* Zrozumiałeś potrzebę bezpieczeństwa fizycznego. Fizyczne bezpieczeństwo jest konieczne, aby zapobiec nieuprawnionemu dostępowi do budynku lub systemu komputerowego, kradzieży danych, uszkodzeniu danych przechowywanych w systemie oraz utracie danych lub uszkodzeniu systemów spowodowanym przyczynami naturalnymi.