Zwiększenie bezpieczeństwa fizycznego

Możesz pokusić się o pominięcie tej części - w końcu czytasz to, aby dowiedzieć się o cyberbezpieczeństwie, a nie o bezpieczeństwie fizycznym. Ale nie rób tego. Pewne aspekty bezpieczeństwa fizycznego są niezbędnymi składnikami każdego programu bezpieczeństwa cybernetycznego, zarówno formalnego, jak i nieformalnego. W rzeczywistości zaledwie kilkadziesiąt lat temu zespoły odpowiedzialne za ochronę komputerów i przechowywanych w nich danych skupiały się w szczególności na bezpieczeństwie fizycznym. Zamknięcie komputera w bezpiecznym miejscu, do którego dostęp miał tylko upoważniony personel, często wystarczało, aby zabezpieczyć go i jego zawartość. Oczywiście pojawienie się sieci i ery Internetu w połączeniu z masowym rozpowszechnianiem się urządzeń komputerowych całkowicie zmieniło ryzyko. Obecnie miliardy ludzi na całym świecie nadal mogą uzyskać elektroniczny dostęp do komputerów zablokowanych w fizycznej lokalizacji. To powiedziawszy, potrzeba bezpieczeństwa fizycznego jest tak samo ważna jak zawsze. W tym rozdziale omówiono elementy bezpieczeństwa fizycznego, które są niezbędne do wdrożenia i zapewnienia odpowiedniego bezpieczeństwa cybernetycznego. Omawiam „co i dlaczego", które musisz wiedzieć o fizycznym bezpieczeństwie, aby zapewnić sobie cyberbezpieczeństwo. Ignorowanie pojęć omawianych w tym rozdziale może narazić Cię na ryzyko naruszenia danych równoważnego lub nawet gorszego niż naruszenie dokonane przez hakerów.

Zrozumienie, dlaczego bezpieczeństwo fizyczne ma znaczenie

Bezpieczeństwo fizyczne oznacza ochronę czegoś przed nieuprawnionym dostępem fizycznym, czy to człowieka, czy natury. Przykładem bezpieczeństwa fizycznego jest trzymanie komputera zamkniętego w szafie serwerowej w biurze, aby uniemożliwić innym manipulowanie przy nim. Celem bezpieczeństwa fizycznego jest zapewnienie bezpiecznego środowiska dla ludzi i majątku osoby, rodziny lub organizacji. W kontekście cyberbezpieczeństwa celem bezpieczeństwa fizycznego jest zapewnienie tego cyfrowemu systemowi i danym, które nie są zagrożone ze względu na sposób, w jaki są fizycznie przechowywane.

Informacje niejawne zawierają tajemnice, których ujawnienie może zagrozić agentom i operacjom amerykańskiego wywiadu, operacji dyplomatycznych i wojskowych i szkodzić bezpieczeństwu narodowemu. Mam nadzieję, że nie przechowujesz w domu bardzo poufnych plików niejawnych.

Jeśli tak, to lepiej, żebyś wiedział o wiele więcej o bezpieczeństwie informacji, niż jest to nauczane w tej książce; ponieważ usunięcie informacji niejawnych z ich właściwego miejsca przechowywania jest często poważnym przestępstwem, proponuję znaleźć sobie dobrego prawnika. (Zobacz poboczny pasek boczny „Problem z pocztą e-mail Sekretarza Stanu Hillary Clinton"). Niemniej jednak zakładam, że masz dane, które chcesz, aby były poufne, dostępne i wolne od korupcji. Mogą one nie być klasyfikowane w rządowym rozumieniu, ale dla Ciebie jego prywatność może mieć kluczowe znaczenie.

Biorąc ekwipunek

Przed wdrożeniem planu ochrony fizycznej musisz zrozumieć, co musisz zabezpieczyć. Prawdopodobnie posiadasz więcej niż jeden typ urządzenia elektronicznego i dane, które różnią się znacznie pod względem poziomu poufności i wrażliwości, które do niego przypisujesz. Pierwszym krokiem we wdrażaniu odpowiedniego zabezpieczenia fizycznego jest zrozumienie, jakie dane i systemy posiadasz, oraz określenie, jakiego poziomu bezpieczeństwa każdy z nich wymaga. Najprawdopodobniej Twoje urządzenia komputerowe dzielą się na dwie kategorie:

* Urządzenia stacjonarne, takie jak komputer stacjonarny siedzący w pokoju rodzinnym, na którym nastolatki grają w gry wideo

* Urządzenia mobilne, takie jak laptopy, tablety i telefony komórkowe

Nie zapomnij spisać sprzętu, do którego podłączone są Twoje urządzenia. Podczas inwentaryzacji urządzeń zwróć uwagę na sieci i sprzęt sieciowy. Do jakich sieci podłączone są urządzenia stacjonarne? Ile sieci jest na miejscu? Gdzie łączą się ze światem zewnętrznym? Gdzie znajduje się odpowiedni sprzęt sieciowy? Z jakimi urządzeniami mobilnymi łączą się bezprzewodowo?

Urządzenia stacjonarne

Urządzenia stacjonarne, takie jak komputery stacjonarne, sprzęt sieciowy i wiele urządzeń Internetu rzeczy (IoT), takich jak kamery przewodowe, to urządzenia, które nie przemieszczają się regularnie z miejsca na miejsce. Urządzenia te mogą oczywiście zostać skradzione, uszkodzone lub niewłaściwie użyte, a zatem muszą być odpowiednio chronione. Dlatego uszkodzenia nie muszą być celowe, dlatego należy je odpowiednio chronić

Uszkodzenia nie muszą być celowe - na początku swojej kariery pomogłem rozwiązać problem z serwerem, który pojawił się, gdy nocny opiekun odłączył niewłaściwie zabezpieczony serwer od zasilacza awaryjnego w celu podłączenia odkurzacza. Tak poważnie. Ponieważ konieczne jest zabezpieczenie urządzeń stacjonarnych w miejscach, w których „mieszkają", należy je inwentaryzować. Zabezpieczenie czegoś, o czym nie wiesz, że posiadasz, jest trudne, jeśli nie niemożliwe. W wielu przypadkach każdy, kto ma fizyczny dostęp do komputera lub innego urządzenia elektronicznego, może uzyskać dostęp do wszystkich danych i programów na tym urządzeniu, niezależnie od stosowanych systemów bezpieczeństwa. Jedyne pytanie dotyczy tego, ile czasu zajmie tej stronie uzyskanie nieautoryzowanego dostępu, którego pragnie. Nieważne, że każdy, kto ma dostęp do urządzenia, może je fizycznie uszkodzić - czy to fizycznie uderzając w nie, wysyłając do niego potężny wzrost mocy, wylewając na nie wodę, czy też podpalając. Jeśli uważasz, że te scenariusze są naciągane, wiedz, że widziałem wszystkie cztery z tych opcji używane przez ludzi, których celem jest uszkodzenie komputerów.

Urządzenia mobilne

Urządzenia mobilne to skomputeryzowane urządzenia, które są często przenoszone. Laptopy, tablety i smartfony to wszystkie urządzenia mobilne. Pod pewnymi względami urządzenia mobilne są z natury bezpieczniejsze niż urządzenia stacjonarne - prawdopodobnie zawsze masz przy sobie telefon komórkowy, więc nie siedzi on w domu bez nadzoru przez długi czas, jak może to być komputer. To powiedziawszy, w rzeczywistości doświadczenie pokazuje, że przenośność radykalnie zwiększa szanse na zgubienie lub kradzież urządzenia. W rzeczywistości pod pewnymi względami urządzenia mobilne są koszmarem specjalistów ds. Bezpieczeństwa. „Smartfon" w Twojej kieszeni jest stale połączony z niezabezpieczoną siecią (Internetem), zawiera bardzo poufne dane, ma tokeny dostępu do Twojej poczty e-mail, mediów społecznościowych i całego szeregu innych ważnych kont, prawdopodobnie brakuje mu wyrafinowanego oprogramowania zabezpieczającego czyli na komputerach stacjonarnych, często znajduje się w miejscach, w których może zostać skradziony, często jest poza zasięgiem wzroku, jest zabierany na wycieczki, które powodują odejście od normalnej rutyny i tak dalej. Właściwa inwentaryzacja każdego urządzenia mobilnego, aby można było odpowiednio zabezpieczyć wszystkie takie urządzenia, ma kluczowe znaczenie.

Lokalizowanie wrażliwych danych

Sprawdź, jakie dane przechowują Twoje urządzenia. Pomyśl o najgorszych konsekwencjach, jeśli nieupoważniona osoba uzyska Twoje dane lub wycieknąą one do opinii publicznej w Internecie. Żadna

lista elementów do wyszukania nie obejmuje wszystkich możliwych scenariuszy, ale oto kilka rzeczy do przemyślenia. Czy masz

* Prywatne zdjęcia i filmy

* Nagrania twojego głosu

* Obrazy twojego pisma ręcznego (szczególnie twojego podpisu)

*Księgi finansowe

*Dokumentacja medyczna

* Dokumenty szkolne

* Listy haseł

* Repozytoria kluczy cyfrowych

* Dokumenty zawierające:

* Numery kart kredytowych

* Numery SSN / EIN / numery identyfikacyjne podatnika

* Nazwiska panieńskie

* Kody do zamków fizycznych lub innych kodów dostępu

* Korespondencja z IRS i krajowymi organami podatkowymi

* Informacje związane z pozwem

* Informacje związane z zatrudnieniem

*Nazwisko rodowe Matki

* Daty urodzenia

* Numery paszportów

* Numery prawa jazdy

* Informacje o twoich pojazdach

* Informacje o Twoich poprzednich adresach

* Dane biometryczne (odciski palców, skan siatkówki, geometria twarzy, dynamika klawiatury i tak dalej)

Elementy te będą musiały być chronione przed cyberzagrożeniami. Ale magazyny danych, w których się znajdują, również muszą być chronione fizycznie, jak opisano w następnej sekcji.

Tworzenie i wykonywanie planu ochrony fizycznej

Aby odpowiednio fizycznie chronić technologię i dane, nie należy próbować po prostu wdrażać różnych kontroli bezpieczeństwa na zasadzie ad hoc. O wiele lepiej jest raczej opracować i wdrożyć plan ochrony fizycznej - dzięki temu unikniesz kosztownych błędów. W większości przypadków fizyczne zabezpieczenie systemów komputerowych polega na zastosowaniu dobrze znanej, ugruntowanej zasady zapobiegania przestępczości, znanej jako Zapobieganie przestępczości poprzez projektowanie

środowiskowe (CPTD), która stanowi, że można zmniejszyć prawdopodobieństwo popełnienia niektórych przestępstw, jeśli stworzysz fizyczny środowisko, które pozwala uprawnionym użytkownikom czuć się bezpiecznie, ale sprawia, że źle postępujący nie są w stanie dostosować się do faktycznego wykonywania planowanych problematycznych działań. Zrozumienie tej ogólnej koncepcji może pomóc w przemyśleniu sposobów zapewnienia bezpieczeństwa własnych systemów i danych. Trzy elementy zapobiegania przestępczości poprzez projektowanie, które mają zastosowanie w ogólnych zasadach zapobiegania przestępczości obejmują kontrolę dostępu, nadzór i oznaczanie:

* Kontrola dostępu: ograniczenie dostępu do uprawnionych stron poprzez stosowanie ogrodzeń, monitorowanych wejść i wyjść, odpowiedniego zagospodarowania terenu itp. Utrudnia przestępcom penetrację budynku lub innego obiektu oraz zwiększa ryzyko oszustów, że zostaną zauważeni, zniechęcając w ten sposób potencjalnych przestępców do faktycznego popełniania przestępstw.

* Nadzór: Przestępcy często unikają popełnienia przestępstw, które prawdopodobnie zostaną zauważone i zarejestrowane; jako takie, oddalają się od środowisk, o których wiedzą, że są dobrze obserwowane. Kamery, osłony i oświetlenie wrażliwe na ruch zniechęcają do przestępstw.

* Oznakowanie: Przestępcy mają tendencję do unikania obszarów, które są wyraźnie oznaczone jako należące do kogoś innego - na przykład za pomocą ogrodzeń i znaków - ponieważ nie chcą się wyróżniać i być łatwo zauważalni podczas popełniania przestępstw. Podobnie unikają środowisk, w których zaznaczane są osoby upoważnione. Weźmy na przykład pod uwagę, że osoba nieupoważniona, która nie nosi munduru pocztowego, spacerując po obszarze oznaczonym „Tylko pracownicy poczty USA", jest znacznie bardziej narażona na zauważenie i zatrzymanie niż ktoś inny chodzący w podobnym nieoznakowanym środowisku należącym do biznes, który nie wymaga mundurów.

Możesz zastosować te same zasady w swoim domu - na przykład umieszczenie komputera w domowym biurze rodzica powoduje wysłanie wiadomości do dzieci, opiekunek i gości, że urządzenie jest poza zasięgiem, o wiele silniejszej niż wiadomość byłaby dostarczona, gdyby ta sama maszyna znajdowały się w pokoju rodzinnym lub legowisku. Podobnie ciekawska opiekunka do dzieci lub gość w domu jest znacznie mniej prawdopodobne, że wejdzie do prywatnego biura bez pozwolenia po tym, jak ktoś mu tego zabroni, jeśli wie, że obszar jest monitorowany za pomocą kamer. Znasz swoje środowisko. Stosując te koncepcje, możesz zwiększyć prawdopodobieństwo, że osoby nieupoważnione nie będą próbowały uzyskać nieautoryzowanego dostępu do Twoich komputerów i danych.

Wdrażanie bezpieczeństwa fizycznego

Możesz użyć wielu technik i technologii, aby zabezpieczyć obiekt lub obiekt. To, ile zabezpieczeń fizycznych wdrażasz dla urządzenia, zależy w dużej mierze od celu, do którego jest ono używane i jakie typy informacji zawiera. Oto kilka przykładów metod zabezpieczania urządzeń - w oparciu o poziom tolerancji ryzyka i budżet możesz wybrać warianty wszystkich, niektórych lub żadnej z tych technik:

* Zamki: Na przykład przechowuj urządzenia w zamkniętym pomieszczeniu, z dostępem do pokoju tylko dla tych osób, które muszą korzystać z urządzenia.W niektórych środowiskach możesz nagrywać lub monitorować wszystkie wejścia i wyjścia z pomieszczenia. Innym popularnym wariantem jest przechowywanie laptopów w sejfie znajdującym się w głównej sypialni lub biurze domowym, gdy komputery nie są używane.

* Kamery wideo: rozważ na przykład ustawienie kamery wideo skoncentrowanej na urządzeniach, aby zobaczyć, kto uzyskuje do nich dostęp i kiedy to robi.

* Ochroniarze: Oczywiście strażnicy nie są praktycznym rozwiązaniem w większości środowisk domowych, ale obrońcy mają czas i miejsce. Na przykład rozważ umieszczenie strażników wewnątrz

pomieszczenia, w którym znajduje się urządzenie, na zewnątrz pomieszczenia, w korytarzach wokół wejścia do pomieszczenia, na zewnątrz budynku i poza jego obwodem.

* Alarmy: Alarmy nie tylko służą jako reaktywna siła, która odstrasza przestępców, którzy faktycznie próbują wejść do domu lub biura, ale również służą jako silny środek odstraszający, zmuszając wielu oportunistycznych złoczyńców do „szukania gdzie indziej" i kierowania na kogoś innego.

* Zabezpieczenie obwodowe: słupki drogowe zapobiegają zderzaniu samochodów z obiektem, a odpowiednie ogrodzenia i ściany uniemożliwiają zbliżanie się ludzi do domu lub budynku biurowego. Należy pamiętać, że większość ekspertów uważa, że ogrodzenie o wysokości poniżej 8 stóp nie zapewnia żadnej znaczącej wartości bezpieczeństwa, jeśli chodzi o potencjalnych intruzów.

* Oświetlenie: Przestępcy unikają dobrze oświetlonych miejsc. Oświetlenie wyzwalane ruchem jest jeszcze bardziej odstraszające niż oświetlenie statyczne. Kiedy nagle zapalają się światła, ludzie w okolicy częściej odwracają się i patrzą na to, co się właśnie stało - i widzą przestępcę dokładnie tak, jak jest oświetlony.

* Ograniczanie ryzyka środowiskowego: jeśli znajdujesz się na obszarze, który może być dotkniętym przez powodzie, upewnić się, że zasoby obliczeniowe są stacjonarne w miejscu, które prawdopodobnie nie zostanie zalane. Jeśli taka rada wydaje się oczywista, weź pod uwagę, że mieszkańcy północnego New Jersey stracili dostęp do telefonu po burzy pod koniec lat 90. XX wieku, kiedy to nastąpiło zalanie aparatury przełączającej - ponieważ znajdowała się ona w piwnicy budynku stojącego nad rzeką. Właściwa ochrona przed pożarami jest kolejnym krytycznym elementem ograniczania ryzyka środowiskowego.

* Zasilanie rezerwowe i sytuacje awaryjne w przypadku awarii zasilania: awarie zasilania mają wpływ nie tylko na komputery, ale także na wiele systemów bezpieczeństwa.

* Nieprzewidziane sytuacje podczas remontów i innych prac budowlanych itp .: Często pomija się zagrożenia dla danych i komputerów podczas remontów domów. Pozostawienie telefonu komórkowego bez nadzoru, gdy pracownicy regularnie wchodzą i wychodzą, na przykład, może być receptą na skradzione urządzenie i / lub ujawnienie danych w urządzeniu.

* Zagrożenia związane z kopiami zapasowymi: Pamiętaj, aby chronić kopie zapasowe danych przy użyciu tych samych środków ostrożności, co w przypadku oryginalnych kopii danych. Poświęcanie czasu i pieniędzy na ochronę komputera za pomocą sejfu i kamer ze względu na dane na jego dysku twardym, na przykład, jest głupie, jeśli pozostawiasz kopie zapasowe tych samych danych na przenośnych dyskach twardych przechowywanych na półce w pokoju rodzinnym w zasięgu wzroku każdego odwiedzającego Twój dom.

Oczywiście powyższa lista nie jest wyczerpująca. Ale jeśli pomyślisz o tym, jak możesz zastosować każdy z tych elementów, aby pomóc chronić swoje urządzenia w kontekście podejścia CPTD, prawdopodobnie skorzystasz ze znacznie większych szans na wystąpienie „niefortunnego incydentu", niż gdybyś tego nie zrobił.

Bezpieczeństwo urządzeń mobilnych

Oczywiście urządzenia mobilne - czyli komputery, tablety, smartfony i inne urządzenia elektroniczne, które są regularnie przenoszone z miejsca na miejsce - stanowią dodatkowe zagrożenie, ponieważ można je łatwo zgubić lub ukraść. W związku z tym, jeśli chodzi o urządzenia mobilne, należy dodać jedną prostą, ale niezwykle ważną, fizyczną zasadę bezpieczeństwa: trzymaj urządzenia w zasięgu wzroku lub zamknięte. Taka rada może wydawać się oczywista; Niestety, ogromna liczba urządzeń jest

kradziona każdego roku, gdy są pozostawione bez opieki, więc możesz być pewien, że urządzenia są kradzione każdego roku, gdy są pozostawione bez opieki, dzięki czemu możesz mieć pewność, że rada nie jest oczywista lub nie jest przestrzegana - i w obu przypadkach chcesz go internalizować i podążać za nim. Oprócz oglądania przez telefon, tablet lub laptop, należy włączyć rozgłaszanie lokalizacji, zdalne wyzwalanie alarmów i zdalne czyszczenie - wszystko to może być nieocenione w szybkim zmniejszaniu ryzyka związanego z zgubieniem lub kradzieżą urządzenia. Niektóre urządzenia oferują nawet funkcję fotografowania lub nagrywania wideo każdego, kto używa urządzenia mobilnego po tym, jak użytkownik oznaczy je jako skradzione - co może nie tylko pomóc w zlokalizowaniu urządzenia, ale także złapać złodziei zaangażowanych w jego kradzież.

Uświadomienie sobie, że osoby wtajemniczone stanowią największe ryzyko

Według większości ekspertów większość incydentów związanych z bezpieczeństwem informacji wiąże się z zagrożeniami wewnętrznymi - co oznacza, że największym zagrożeniem dla firm są ich pracownicy. Podobnie, jeśli dzielisz komputer domowy z członkami rodziny, którzy są mniej świadomi cyberprzestrzeni, mogą stanowić największe zagrożenie dla twojego cyberbezpieczeństwa. Możesz bardzo dbać o swój komputer, ale jeśli nastolatek pobierze na urządzenie oprogramowanie zainfekowane złośliwym oprogramowaniem, możesz spotkać się z niemiłą niespodzianką. Jedna krytyczna zasada z „dawnych czasów", która brzmi dzisiaj prawdziwa - mimo że często jest odrzucana jako przestarzała ze względu na wykorzystanie technologii takich jak szyfrowanie - oznacza, że każdy, kto może fizycznie uzyskać dostęp do komputera, może mieć dostęp do danych na tym komputerze. Zasada ta obowiązuje nawet w przypadku korzystania z szyfrowania, z co najmniej dwóch powodów: Ktoś, kto uzyskuje dostęp do Twojego urządzenia, może nie mieć dostępu do Twoich danych, ale z pewnością może je zniszczyć, a nawet uzyskać do nich dostęp z jednego lub więcej z następujących powodów:

* Możliwe, że nie skonfigurowałeś poprawnie szyfrowania.

* Twój komputer może mieć podatną na wykorzystanie lukę.

* Oprogramowanie szyfrujące może mieć błąd, który osłabia jego zdolność do właściwej ochrony twoich tajemnic.

* Ktoś mógł uzyskać hasło do odszyfrowania.

* Ktoś może chcieć skopiować Twoje dane i poczekać, aż komputery będą wystarczająco wydajne, aby złamać szyfrowanie.

Oto podsumowanie: jeśli nie chcesz, aby ludzie mieli dostęp do danych, nie tylko zabezpiecz je logicznie (na przykład szyfrowaniem), ale także zabezpiecz je fizycznie, aby uniemożliwić im uzyskanie kopii danych, nawet w postaci zaszyfrowanej. W związku z tym, jeśli Twój komputer zawiera pliki, do których nie chcesz, aby Twoje dzieci miały dostęp, nie udostępniaj swojego komputera swoim dzieciom. Nie polegaj wyłącznie na bezpieczeństwie cyfrowym. Wykorzystaj obronę fizyczną. Chociaż prawdą jest, że sprytne, zdolne dzieci mogą włamać się do twojego komputera w sieci LAN, ryzyko takiego ataku jest niewielkie w porównaniu z pokusą ciekawskiego dziecka, które faktycznie korzysta z twojego komputera. To powiedziawszy, najlepiej byłoby trzymać najbardziej wrażliwe dane i maszyny w sieci fizycznie odizolowanej od sieci używanej przez dzieci.