Zabezpieczanie małej firmy

Prawie wszystko, o czym mówimy , dotyczy zarówno osób fizycznych, jak i firm. Właściciele małych firm i pracownicy powinni zdawać sobie sprawę z innych kwestii, które niekoniecznie muszą być ważne dla poszczególnych osób. W tym rozdziale omówiono niektóre z tych zagadnień związanych z cyberbezpieczeństwem. Mógłbym napisać całą serię książek o poprawie cyberbezpieczeństwa małych firm. W związku z tym ten rozdział nie jest wyczerpującą listą wszystkiego, co musi wiedzieć każda mała firma. Raczej daje do myślenia osobom prowadzącym małe firmy.

Upewnianie się, że ktoś tu rządzi

Poszczególne osoby w domu są odpowiedzialne za bezpieczeństwo swoich komputerów, ale co się dzieje, gdy masz sieć i wielu użytkowników? Ktoś w firmie musi ostatecznie „wziąć na siebie" odpowiedzialność za bezpieczeństwo informacji. Tą osobą możesz być Ty, właściciel firmy lub ktoś inny. Ale ktokolwiek jest odpowiedzialny, musi jasno zrozumieć, że jest odpowiedzialny. W wielu przypadkach małych firm osoba odpowiedzialna za bezpieczeństwo informacji zleca niektóre codzienne czynności na zewnątrz. Mimo to ta osoba jest ostatecznie odpowiedzialna za zapewnienie, że niezbędne działania, takie jak instalowanie poprawek bezpieczeństwa, będą się odbywać i odbywać się na czas. Jeśli dojdzie do naruszenia, stwierdzenie, że „myślałem, że taki a taki zadbał o tę funkcję bezpieczeństwa" nie jest wymówką, która będzie miała duże znaczenie.

Uważając na pracowników

Pracownicy i wiele zagrożeń dla cyberbezpieczeństwa, które stwarzają, może stać się głównym problemem dla małych firm. Błędy ludzkie są głównym katalizatorem naruszeń danych.Nawet jeśli czytasz tę książkę i starasz się poprawić swoją wiedzę i postawę w zakresie cyberbezpieczeństwa, Twoi pracownicy i współpracownicy mogą nie wykazywać takiego samego zaangażowania jak Ty, jeśli chodzi o ochronę dane i systemy. W związku z tym jedną z najważniejszych rzeczy, które może zrobić właściciel małej firmy, jest edukowanie swoich pracowników. Edukacja składa się zasadniczo z trzech niezbędnych elementów:

* Świadomość zagrożeń: musisz upewnić się, że każdy pracownik pracujący dla firmy rozumie, że on lub ona i cała firma są celami. Ludzie, którzy uważają, że przestępcy chcą włamać się do ich komputerów, telefonów i baz danych, zachowują się inaczej niż ludzie, którzy nie zinternalizowali tej rzeczywistości. Podczas gdy formalne, regularne szkolenia są idealne, nawet pojedyncza, krótka rozmowa prowadzona na początku pracy i odświeżana okresowymi przypomnieniami może przynieść znaczną wartość w tym zakresie.

* Podstawowe szkolenie w zakresie bezpieczeństwa informacji: wszyscy pracownicy powinni rozumieć pewne podstawy bezpieczeństwa informacji. Powinni na przykład wiedzieć, jak unikać cyber-ryzykownych zachowań, takich jak otwieranie załączników i klikanie linków znajdujących się w nieoczekiwanych wiadomościach e-mail, pobieranie muzyki lub filmów z wątpliwych źródeł, niewłaściwe korzystanie z publicznej sieci Wi-Fi do zadań wrażliwych lub kupowanie produktów od nieznane sklepy z cenami zbyt dobrymi, aby mogły być prawdziwe "i bez publicznie znanego adresu fizycznego. (Zobacz rozdział 20, aby uzyskać wskazówki dotyczące bezpiecznego korzystania z publicznej sieci Wi-Fi). Liczne powiązane materiały szkoleniowe (często bezpłatne) są dostępne w Internecie. To powiedziawszy, nigdy nie polegaj na samym treningu, który służy jako jedyna linia obrony przed jakimkolwiek znaczącym ryzykiem dla ludzi. Wiele osób robi głupie rzeczy, nawet po otrzymaniu jasnego przeszkolenia, aby było inaczej. Ponadto szkolenie nie dotyczy nieuczciwych pracowników, którzy celowo sabotują bezpieczeństwo informacji.

* Praktyka: Szkolenie z zakresu bezpieczeństwa informacji nie powinno mieć charakteru teoretycznego. Pracownicy powinni mieć możliwość przećwiczenia tego, czego się nauczyli, na przykład poprzez zidentyfikowanie i usunięcie / zgłoszenie testowego e-maila phishingowego.

Zachęcaj pracowników

Tak jak powinieneś pociągać pracowników do odpowiedzialności za ich działania, tak jak powinieneś pociągać pracowników do odpowiedzialności za ich działania, jeśli coś pójdzie nie tak, powinieneś również nagradzać pracowników za wykonywanie ich pracy w sposób cyberbezpieczny i działanie z odpowiednią cyberhigieną. Pozytywne wzmocnienie może wiele zdziałać i prawie zawsze jest lepiej odbierane niż negatywne. Ponadto wiele organizacji z powodzeniem wdrożyło systemy raportowania, które umożliwiają pracownikom anonimowe powiadamianie odpowiednich organów w branży o podejrzanych działaniach poufnych, które mogą wskazywać na zagrożenie, a także o potencjalnych błędach w systemach, które mogą prowadzić do luk w zabezpieczeniach. Takie programy są powszechne w większych firmach, ale mogą przynieść korzyści również wielu małym firmom.

Unikaj wydawania kluczy do zamku

Istnieje niezliczona ilość historii o pracownikach popełniających błędy, które otwierają organizacyjne drzwi hakerom oraz o niezadowolonych pracownikach kradnących dane i / lub sabotujących systemy. Szkody spowodowane takimi incydentami mogą być katastrofalne dla małej firmy. Chroń siebie i swoją firmę przed tego typu zagrożeniami, konfigurując infrastrukturę informacyjną tak, aby powstrzymała szkody, jeśli coś pójdzie nie tak. Jak możesz to robić? Zapewnij pracownikom dostęp do wszystkich systemów komputerowych i danych, których potrzebują, aby wykonywać swoją pracę z maksymalną wydajnością, ale nie dawaj im dostępu do niczego innego, co ma wrażliwy charakter. Na przykład programiści nie powinni mieć dostępu do systemu płacowego firmy, a kontroler nie potrzebuje dostępu do systemu kontroli wersji zawierającego kod źródłowy zastrzeżonego oprogramowania firmy. Ograniczenie dostępu może mieć ogromne znaczenie pod względem zakresu wycieku danych, jeśli pracownik stanie się nieuczciwy. Wiele firm nauczyło się tej lekcji na własnej skórze. Nie stań się jednym z nich.

Daj każdemu własne poświadczenia

Każdy pracownik uzyskujący dostęp do każdego systemu używanego przez organizację powinien mieć własne dane logowania do tego systemu. Nie udostępniaj danych logowania! Wdrożenie takiego schematu poprawia możliwość audytu działań ludzi (co może być konieczne, jeśli dojdzie do naruszenia danych lub innego zdarzenia związanego z cyberbezpieczeństwem), a także zachęca ludzi do lepszej ochrony swoich haseł, ponieważ wiedzą, że jeśli konto jest nadużywane, kierownictwo zajmie się sprawą z nimi osobiście, a nie z zespołem. Świadomość, że dana osoba zostanie pociągnięta do odpowiedzialności za swoje zachowanie związane z utrzymaniem lub naruszaniem bezpieczeństwa może zdziałać cuda w proaktywnym sensie. Podobnie każda osoba powinna mieć własne możliwości uwierzytelniania wieloskładnikowego - niezależnie od tego, czy będzie to fizyczny token, kod wygenerowany na jej smartfonie itp.

Ogranicz administratorów

Administratorzy systemu zwykle mają uprawnienia superużytkownika, co oznacza, że mogą mieć dostęp, czytać, usuwać i modyfikować dane innych osób. Dlatego ważne jest, aby jeśli Ty - właściciel firmy - nie jesteś jedynym superużytkownikiem, wdrożysz mechanizmy kontrolne, aby monitorować działania administratora. Na przykład możesz rejestrować działania administratora na oddzielnym komputerze, do którego administrator nie ma dostępu. Zezwolenie na dostęp tylko z określonej

maszyny w określonej lokalizacji - co czasami jest niemożliwe ze względu na potrzeby biznesowe - jest innym podejściem, ponieważ umożliwia skierowanie kamery na tę maszynę, aby nagrywać wszystko, co robi administrator.

Ogranicz dostęp do kont firmowych

Twoja firma może mieć kilka własnych kont. Na przykład może mieć konta w mediach społecznościowych - stronę na Facebooku, konto na Instagramie i konto na Twitterze - obsługę klienta, konta e-mail, konta telefoniczne i inne konta narzędziowe. Udziel dostępu tylko tym osobom, które absolutnie potrzebują dostępu do tych kont (patrz poprzednia sekcja). Idealnie byłoby, gdyby każda osoba, której dajesz dostęp, miała dostęp podlegający audytowi - to znaczy, że powinno być łatwe do ustalenia, kto co zrobił z kontem. Podstawowa kontrola i słyszalność są łatwe do osiągnięcia, jeśli chodzi na przykład o strony na Facebooku, ponieważ możesz być właścicielem strony na Facebooku dla firmy, jednocześnie zapewniając innym osobom możliwość pisania na stronie. Jednak w niektórych innych środowiskach szczegółowe kontrole nie są dostępne i będziesz musiał zdecydować, czy udostępnić wiele osób logujących się na konto w mediach społecznościowych, czy też pozwolić im przesyłać treści do jednej osoby (być może nawet Ty), kto tworzy odpowiednie posty. Wyzwanie polegające na zapewnieniu każdemu autoryzowanemu użytkownikowi korporacyjnych kont mediów społecznościowych własnego konta, aby uzyskać zarówno kontrolę, jak i słyszalność pogarsza fakt, że wszystkie wrażliwe konta powinny być chronione za pomocą uwierzytelniania wieloskładnikowego. Niektóre systemy oferują funkcje uwierzytelniania wieloskładnikowego, które uwzględniają fakt, że wielu niezależnych użytkowników może wymagać przyznania podlegającego audytowi dostępu do jednego konta. Jednak w niektórych przypadkach systemy, które oferują funkcje uwierzytelniania wieloskładnikowego, nie pasują dobrze do środowisk wieloosobowych. Mogą np. Dopuszczać tylko jeden numer telefonu komórkowego, na który hasła jednorazowe są przesyłane SMS-em. W takich scenariuszach musisz zdecydować, czy:

* Użyć uwierzytelniania wieloskładnikowego, ale z obejściem - na przykład używając numeru VOIP do odbierania SMS-ów i konfigurując numer VOIP do przekazywania wiadomości do wielu stron za pośrednictwem poczty elektronicznej (co jest oferowane bezpłatnie, na przykład , przez Google Voice).

* Korzystać z uwierzytelniania wieloskładnikowego bez obejścia - i skonfiguruj urządzenia autoryzowanych użytkowników tak, aby nie wymagały uwierzytelniania wieloskładnikowego dla wykonywanych przez nich czynności. Nie używaj uwierzytelniania wieloskładnikowego, ale polegaj wyłącznie na silnych hasłach (niezalecane).

* Znaleźć inne obejście, modyfikując swoje procesy, procedury lub technologie używane w celu uzyskania dostępu do takich systemów.

* Korzystaj z produktów innych firm, które nakładają się na systemy (często najlepsza opcja, jeśli jest dostępna).

Ostatnia opcja jest często najlepszą opcją. Na przykład różne systemy zarządzania treścią pozwalają na konfigurację dla wielu użytkowników, z których każdy ma własne niezależne, silne możliwości uwierzytelniania, a wszyscy tacy użytkownicy mają podlegający kontroli dostęp do jednego konta w mediach społecznościowych.

Podczas gdy większe przedsiębiorstwa prawie zawsze stosują jakiś wariant ostatniego podejścia - zarówno ze względów zarządzania, jak i bezpieczeństwa - wiele małych firm ma tendencję do wybierania łatwych rozwiązań i po prostu nie stosuje silnego uwierzytelniania w takich przypadkach. Koszt wdrożenia odpowiednich zabezpieczeń - zarówno w dolarach, jak i czasie - jest zwykle dość niski,

dlatego zdecydowanie warto zbadać produkty innych firm, zanim zdecydujesz się na inne podejście. Wartość posiadania odpowiedniego zabezpieczenia z możliwością audytu stanie się natychmiast jasna, jeśli kiedykolwiek zdarzy się, że zdarzy się, że zdarzy się, że zdarzy się, iż zdarzy się, że zdegustowany pracownik miał dostęp do kont firmowych w mediach społecznościowych lub gdy szczęśliwy i zadowolony pracownik z takim dostępem zostanie zhakowany.

Wdrażanie polityk pracowniczych

Firmy różnej wielkości, które zatrudniają pracowników, potrzebują podręcznika pracowniczego zawierającego szczegółowe zasady dotyczące korzystania przez pracowników z systemów i danych technologii biznesowej. Omówienie wszystkich elementów podręczników dla pracowników wykracza poza zakres tej książki, ale poniżej przedstawiono przykłady zasad, które firmy mogą wdrożyć w celu zarządzania wykorzystaniem zasobów technologicznych firmy:

* Od pracowników firmy oczekuje się odpowiedzialnego, odpowiedniego i produktywnego korzystania z technologii, jeśli jest to konieczne do wykonywania ich obowiązków zawodowych.

* Korzystanie z firmowych urządzeń, a także firmowego dostępu do Internetu i poczty elektronicznej, które są udostępniane pracownikowi przez firmę, służy do wykonywania czynności związanych z pracą. Minimalny użytek osobisty jest dopuszczalny, pod warunkiem, że używanie go jako takiego przez pracownika nie narusza żadnych innych zasad opisanych w tym dokumencie i nie koliduje z jego pracą.

* Każdy pracownik jest odpowiedzialny za sprzęt komputerowy i oprogramowanie dostarczone mu przez firmę, w tym za zabezpieczenie takich przedmiotów przed kradzieżą, utratą lub uszkodzeniem.

* Każdy pracownik jest odpowiedzialny za swoje rachunki udostępnione przez firmę, w tym za zabezpieczenie dostępu do kont. * Pracownikom surowo zabrania się udostępniania jakichkolwiek dostarczonych przez firmę przedmiotów służących do uwierzytelniania (haseł, sprzętowych urządzeń uwierzytelniających, kodów PIN itp.) I są odpowiedzialni za ich ochronę.

* Pracownikom surowo zabrania się podłączania jakichkolwiek urządzeń sieciowych, takich jak routery, punkty dostępowe, wzmacniacze zasięgu itp., Do sieci firmowych, chyba że zostały do tego wyraźnie upoważnione przez dyrektora generalnego firmy. Podobnie pracownikom surowo zabrania się podłączania jakichkolwiek komputerów osobistych lub urządzeń elektronicznych - w tym jakichkolwiek urządzeń Internetu rzeczy (IoT) - do sieci firmowych innych niż sieć Gość, na warunkach określonych wyraźnie w zasadach „Przynieś własne urządzenie” (BYOD) .

* Pracownicy są odpowiedzialni za upewnienie się, że oprogramowanie zabezpieczające działa na wszystkich urządzeniach dostarczonych przez firmę. Firma zapewni takie oprogramowanie, ale nie ma możliwości sprawdzenia, czy takie systemy zawsze działają zgodnie z oczekiwaniami. Pracownicy nie mogą dezaktywować ani w inny sposób uszkadzać takich systemów bezpieczeństwa i muszą niezwłocznie powiadomić dział IT firmy, jeśli podejrzewają, że jakakolwiek część systemów bezpieczeństwa może zostać naruszona, nie działa lub działa nieprawidłowo.

* Pracownicy są odpowiedzialni za aktualizowanie oprogramowania zabezpieczającego. Wszystkie urządzenia wydane przez firmę są wyposażone w funkcję automatycznej aktualizacji; pracownicy nie mogą wyłączać tej funkcji.

* Podobnie pracownicy są odpowiedzialni za aktualizowanie swoich urządzeń do najnowszego systemu operacyjnego, sterowników i poprawek aplikacji, gdy dostawcy takie poprawki wydają. Wszystkie urządzenia wydane przez firmę są wyposażone w funkcję automatycznej aktualizacji; pracownicy nie mogą wyłączać tej funkcji.

* Wykonywanie jakiejkolwiek nielegalnej działalności - niezależnie od tego, czy dany czyn jest przestępstwem, wykroczeniem lub naruszeniem prawa cywilnego - jest surowo zabronione. Zasada ta ma zastosowanie do prawa federalnego, prawa stanowego i prawa lokalnego w każdym obszarze i w dowolnym czasie, w którym pracownik podlega takim przepisom.

* Materiały chronione prawem autorskim należące do jakiejkolwiek strony innej niż firma lub pracownik nie mogą być przechowywane ani przesyłane przez pracownika na sprzęcie firmy bez wyraźnej pisemnej zgody posiadacza praw autorskich. Materiały, na które firma udzieliła licencji, mogą być przekazywane zgodnie z odpowiednimi licencjami.

* Masowe wysyłanie niechcianych e-maili (spamowanie) jest zabronione. Wykorzystywanie zasobów firmy do wykonywania jakichkolwiek zadań, które są niezgodne z misją firmy - nawet jeśli nie jest to technicznie nielegalne - jest zabronione. Obejmuje to między innymi uzyskiwanie dostępu lub przekazywanie materiałów o charakterze jednoznacznie seksualnym, wulgaryzmów, szerzenie nienawiści, zniesławiających materiałów, dyskryminujące materiały, obrazy lub opisy przemocy, gróźb, cyberprzemocy, materiałów związanych z hakowaniem, materiałów skradzionych itp.

* Poprzednia zasada nie ma zastosowania do pracowników, których praca wymaga pracy z takimi materiałami, tylko w zakresie, w jakim jest to niezbędne do wykonywania obowiązków służbowych. Na przykład pracownicy odpowiedzialni za konfigurację filtru poczty e-mail firmy mogą, bez naruszania poprzedniej zasady, przesyłać sobie e-maile z informacją o dodaniu do konfiguracji filtra różnych terminów związanych z mową nienawiści i wulgarnymi treściami.

* Żadne urządzenie firmowe wyposażone w Wi-Fi lub komórkową komunikację nie może być włączane w Chinach lub Rosji bez wyraźnej pisemnej zgody dyrektora generalnego firmy. Urządzenia wypożyczone zostaną udostępnione pracownikom podróżującym w te regiony. Żadne urządzenie osobiste włączone w tych regionach nie może być podłączone do sieci gościa (ani żadnej innej sieci firmowej).

* Każde użycie publicznej sieci Wi-Fi z urządzeniami firmowymi musi być zgodne z zasadami firmy dotyczącymi publicznych sieci Wi-Fi.

* Pracownicy muszą tworzyć kopie zapasowe swoich komputerów przy użyciu firmowego systemu tworzenia kopii zapasowych, zgodnie z zasadami firmy dotyczącymi tworzenia kopii zapasowych.

* Pracownicy nie mogą kopiować ani w inny sposób tworzyć kopii zapasowych danych z urządzeń firmowych na swoich komputerach osobistych i / lub urządzeniach magazynujących.

* Wszelkie hasła do wszystkich systemów używanych w ramach pracy pracownika muszą być unikalne i nie mogą być ponownie wykorzystywane w żadnym innym systemie. Wszystkie takie hasła muszą składać się z trzech lub więcej słów, z których przynajmniej jedno nie występuje w słowniku języka angielskiego, połączone razem z cyframi lub znakami specjalnymi lub spełniać wszystkie następujące warunki:

-Zawieraj osiem lub więcej znaków z co najmniej jedną wielką literą

-Zawierają co najmniej jedną małą literę

-Zawieraj co najmniej jedną liczbę

-Nie zawiera żadnych słów, które można znaleźć w polskim słowniku

-W obu przypadkach nazwiska krewnych, przyjaciół lub współpracowników nie mogą być używane jako część hasła.

* Dane można wynieść z biura wyłącznie w celach biznesowych i przed usunięciem należy je zaszyfrować. Ta reguła ma zastosowanie niezależnie od tego, czy dane znajdują się na dysku twardym, dysku SSD, CD / DVD, napędzie USB, czy na jakimkolwiek innym nośniku lub są przesyłane przez Internet. Wszelkie takie dane muszą zostać zwrócone do biura (lub według uznania firmy, zniszczone) natychmiast po zakończeniu ich zdalnego wykorzystania lub po rozwiązaniu stosunku pracy przez pracownika, w zależności od tego, co nastąpi wcześniej.

* W przypadku naruszenia lub innego zdarzenia związanego z cyberbezpieczeństwem lub jakiegokolwiek naturalnego lub katastrofy spowodowanej przez człowieka, żaden pracownik inny niż oficjalnie wyznaczony rzecznik firmy nie może przemawiać do mediów w imieniu firmy.

* Żadne urządzenia od żadnego producenta, które FBI lub inne federalne organy ścigania i agencje wywiadowcze w Stanach Zjednoczonych ostrzegły, że ich zdaniem rządy zagraniczne używają do szpiegowania Amerykanów, nie mogą być podłączone do jakiejkolwiek sieci firmowej (w tym sieci dla gości) lub przeniesione do fizycznej biura firmy.

Egzekwowanie zasad dotyczących mediów społecznościowych

Opracowywanie, wdrażanie i egzekwowanie zasad dotyczących mediów społecznościowych jest ważne, ponieważ nieodpowiednie posty w mediach społecznościowych publikowane przez Twoich pracowników (lub Ciebie) mogą wyrządzić różnego rodzaju szkody. Mogą ujawniać poufne informacje, naruszać zasady zgodności i pomagać przestępcom inżynierom społecznym i atakować Twoją organizację, narażać Twoją firmę na bojkot i / lub procesy sądowe i tak dalej. Chcesz wyjaśnić wszystkim pracownikom, jakie jest, a jakie jest niedopuszczalne korzystanie z mediów społecznościowych. W ramach procesu tworzenia zasad rozważ skonsultowanie się z prawnikiem, aby upewnić się, że nie naruszasz niczyjej wolności słowa. Możesz także wdrożyć technologię, aby media społecznościowe nie przekształciły się z platformy marketingowej w koszmar.

Monitorowanie pracowników

Niezależnie od tego, czy planują faktycznie monitorować wykorzystanie technologii przez pracowników, firmy powinny informować użytkowników, że mają do tego prawo. Jeśli pracownik miałby na przykład oszukać i wykraść dane, nie chcesz, aby dopuszczalność dowodów została zakwestionowana na tej podstawie, że nie masz prawa do monitorowania pracownika. Ponadto mówienie pracownikom, że mogą być monitorowani, zmniejsza prawdopodobieństwo, że pracownicy będą robić rzeczy, których nie powinni robić, ponieważ wiedzą, że mogą być monitorowani podczas wykonywania takich czynności. Oto przykład tekstu, który możesz przekazać pracownikom jako część podręcznika pracownika lub podobnego, gdy rozpoczynają pracę:

Firma, według własnego uznania i bez dalszego powiadamiania pracownika, zastrzega sobie prawo do monitorowania, badania, przeglądu, rejestrowania, gromadzenia, przechowywania, kopiowania, przekazywania innym oraz kontrolowania wszelkiej i całej wiadomości e-mail i innych wiadomości elektronicznych, plików, oraz wszelkie inne treści, aktywność sieciową, w tym korzystanie z Internetu, przesyłane przez lub za pośrednictwem jej systemów technologicznych lub przechowywane w jej systemach technologicznych lub systemy, zarówno na miejscu, jak i poza nim. Takie systemy obejmują systemy, których jest właścicielem i które obsługuje, oraz systemy, które dzierżawi, licencjonuje lub do których posiada jakiekolwiek inne prawa użytkowania. Ponadto, niezależnie od tego, czy są wysyłane do strony wewnętrznej, strony zewnętrznej, czy do obu, wszelkie wiadomości e-mail, wiadomości tekstowe i / lub inne wiadomości błyskawiczne, pocztę głosową i / lub wszelkie inne wiadomości elektroniczne są uważane za zapisy biznesowe Firmy i mogą być podlega ujawnieniu w przypadku sporu

sądowego i / lub ujawnieniu na podstawie nakazów wydanych na podstawie spółki lub żądań organów regulacyjnych i innych stron.

Biorąc pod uwagę ubezpieczenie cybernetyczne

Chociaż ubezpieczenie cyberbezpieczeństwa może być przesadą dla większości małych firm, jeśli uważasz, że Twoja firma może ponieść katastrofalną stratę lub nawet całkowicie upaść, jeśli zostanie naruszona, możesz rozważyć zakup ubezpieczenia. Jeśli wybierzesz tę drogę, pamiętaj, że prawie wszystkie polisy ubezpieczeniowe w zakresie cyberbezpieczeństwa mają wyodrębnienia lub wyłączenia - więc upewnij się, że dokładnie rozumiesz, co jest objęte, a co nie, i za jaką kwotę szkody faktycznie jesteś objęty ubezpieczeniem. Jeśli Twoja firma upadnie z powodu naruszenia, polityka, która opłaca się tylko za to, aby ekspert spędził dwie godziny na przywróceniu danych, nie będzie wiele warta. Ubezpieczenie cyberbezpieczeństwa nigdy nie zastąpi właściwego cyberbezpieczeństwa. W rzeczywistości ubezpieczyciele zwykle wymagają, aby firma spełniała określony standard cyberbezpieczeństwa, aby wykupić i utrzymać ochronę. W niektórych przypadkach ubezpieczyciel może nawet odmówić wypłaty roszczenia, jeśli stwierdzi, że ubezpieczony został naruszony przynajmniej w części z powodu zaniedbania ze strony ubezpieczonego lub z powodu nieprzestrzegania przez stronę naruszoną określonych standardów lub praktyk odpowiednią polisą ubezpieczeniową.

Przestrzeganie przepisów i zgodność

Firmy mogą podlegać różnym prawom, zobowiązaniom umownym i standardom branżowym, jeśli chodzi o cyberbezpieczeństwo. Lokalne biuro Small Business Administration może być w stanie udzielić Ci wskazówek, jakie przepisy mogą na Ciebie wpływać. Pamiętaj jednak, że nic nie zastąpi zatrudnienia odpowiednio wyszkolonego prawnika z doświadczeniem w tej dziedzinie prawa, który udzieli profesjonalnej porady zoptymalizowanej pod Twoją konkretną sytuację. W poniższych sekcjach przedstawiono przykłady kilku takich przepisów, norm itp., Które często mają wpływ na małe firmy.

Ochrona danych pracowników

Odpowiadasz za ochronę poufnych informacji na temat swoich pracowników. W przypadku akt fizycznych należy na ogół zabezpieczyć rekordy co najmniej podwójnym ryglowaniem - przechowywanie akt papierowych w zamkniętej szafce w zamkniętym pomieszczeniu (bez używania tego samego klucza do obu). W przypadku plików elektronicznych pliki powinny być przechowywane w postaci zaszyfrowanej w chronionym hasłem folderze, dysku lub dysku wirtualnym. Takie standardy mogą jednak nie być adekwatne w każdej konkretnej sytuacji, dlatego warto skonsultować się z prawnikiem.

Pamiętaj, że brak odpowiedniej ochrony informacji o pracownikach może mieć poważne skutki: jeśli Twoja firma zostanie naruszona, a przestępca uzyska prywatne informacje o pracownikach, pracownicy, których to dotyczy, i byli pracownicy mogą potencjalnie pozwać Ciebie, a rząd może również ukarać Cię grzywną. Koszty środków zaradczych mogą być również znacznie wyższe niż koszty prewencji proaktywnej. Oczywiście wpływ złej reklamy na sprzedaż firmy może być również katastrofalny. Pamiętaj, że akta pracowników, formularze W2, numery ubezpieczenia społecznego, formularze uprawnień do zatrudnienia I9, adresy domowe i numery telefonów, informacje medyczne, rejestry urlopów, urlopów rodzinnych itd. Są potencjalnie uważane za prywatne. Ogólnie rzecz biorąc, jeśli nie masz pewności, czy niektóre informacje można uznać za prywatne, zachowaj ostrożność i traktuj je tak, jakby były prywatne.

PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) to standard bezpieczeństwa informacji dla organizacji obsługujących główne karty kredytowe i związane z nimi informacje. Podczas gdy wszystkie firmy różnej wielkości, które podlegają standardowi PCI DSS, muszą być z nim zgodne, PCI uwzględnia różne poziomy zasobów dostępnych dla firm różnej wielkości. Zgodność z PCI ma efektywnie cztery różne poziomy. Na jakim poziomie organizacja musi mieć zgodność zwykle opiera się głównie na liczbie transakcji kartą kredytową przetwarzanych rocznie. Inne czynniki, takie jak ryzykowne płatności otrzymywane przez firmę, również mają znaczenie. Różne poziomy to:

Poziom PCI 4: Standardy dla firm, które przetwarzają mniej niż 20 000 transakcji kartami kredytowymi rocznie

Poziom PCI 3: Standardy dla firm przetwarzających od 20 000 do 1 000 000 transakcji kartami kredytowymi rocznie

Poziom PCI 2: Standardy dla firm przetwarzających od 1 000 000 do 6 000 000 transakcji kart kredytowych rocznie

Poziom PCI 1: Standardy dla firm przetwarzających ponad 6 000 000 transakcji kartami kredytowymi rocznie

Szczegółowe badanie PCI wykracza poza zakres tej książki. Na ten temat napisano wiele, całych książek. Jeśli prowadzisz małą firmę i przetwarzasz płatności kartą kredytową lub przechowujesz dane karty kredytowej z jakiegokolwiek innego powodu, poproś o pomoc kogoś znającego się na PCI. W wielu przypadkach podmioty przetwarzające Twoje karty kredytowe będą w stanie polecić odpowiedniego konsultanta lub poprowadzić Cię samodzielnie.

Przepisy dotyczące ujawniania naruszeń

W ostatnich latach różne jurysdykcje wprowadziły tak zwane naruszenia przepisy dotyczące ujawniania informacji, które nakładają na firmy obowiązek publicznego ujawnienia, jeśli podejrzewają, że naruszenie mogło zagrozić niektórym rodzajom przechowywanych informacji. Przepisy dotyczące ujawniania naruszeń różnią się znacznie w zależności od jurysdykcji, ale w niektórych przypadkach mogą mieć zastosowanie nawet do najmniejszych firm. Upewnij się, że znasz przepisy dotyczące Twojej firmy. Jeśli z jakiegoś powodu dojdzie do naruszenia, ostatnią rzeczą, jakiej chcesz, jest kara ukarana przez rząd za niewłaściwe potraktowanie naruszenia. Pamiętaj: wiele małych firm upada w wyniku naruszenia; wkroczenie rządu do walki tylko pogarsza szanse przetrwania Twojej firmy. Prawa mające zastosowanie do Twojej firmy mogą obejmować nie tylko przepisy jurysdykcji, w której fizycznie się znajdujesz, ale również jurysdykcje osób, dla których przetwarzasz informacje.

RODO

Ogólne rozporządzenie o ochronie danych (RODO) to europejskie rozporządzenie o ochronie prywatności, które weszło w życie w 2018 r. I ma zastosowanie do wszystkich firm zajmujących się przetwarzaniem danych konsumenckich mieszkańców Unii Europejskiej, bez względu na wielkość, branżę lub kraj pochodzenia firmy i bez względu na to, czy mieszkaniec UE fizycznie znajduje się na terenie UE. Przewiduje surowe kary dla przedsiębiorstw, które nie chronią należycie prywatnych informacji należących do mieszkańców UE. Niniejsze rozporządzenie oznacza, że mała firma w Nowym Jorku, która sprzedaje przedmiot rezydentowi UE znajdującemu się w Nowym Jorku, może podlegać RODO w celu uzyskania informacji o kupującym i teoretycznie może podlegać surowym karom, jeśli nie zapewni odpowiedniej ochrony dane. Na przykład w lipcu 2019 r. Brytyjskie Biuro Komisarza ds. Informacji (ICO) ogłosiło, że zamierza ukarać British Airways około 230 mln USD, a Marriott około 123 mln USD za naruszenia związane z RODO wynikające z naruszeń danych. RODO jest złożone. Jeśli

uważasz, że Twoja firma może podlegać RODO, porozmawiaj z prawnikiem, który zajmuje się takimi sprawami.

Nie panikuj co do RODO. Nawet jeśli mała firma w Stanach Zjednoczonych technicznie podlega RODO, jest mało prawdopodobne, że UE w najbliższym czasie podejmie próbę nałożenia kar na małe amerykańskie firmy, które nie działają w Europie; ma dużo większe ryby do smażenia. To powiedziawszy, nie ignoruj RODO, ponieważ w końcu małe amerykańskie firmy mogą stać się celem działań egzekwujących.

HIPAA

Prawo federalne w Stanach Zjednoczonych wymaga, aby strony przechowujące informacje związane z opieką zdrowotną chroniły je w celu zachowania prywatności osób, których informacje medyczne znajdują się w danych. Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA), która weszła w życie w 1996 r., Przewiduje surowe kary za niewłaściwą obronę takich informacji. Upewnij się, że wiesz, czy ustawa HIPAA ma zastosowanie do Twojej firmy, a jeśli tak, upewnij się, że odpowiednio chronisz dane, do których ma ona zastosowanie, zgodnie ze standardami branżowymi lub lepszymi.

Dane biometryczne

Jeśli korzystasz z jakichkolwiek form uwierzytelniania biometrycznego lub z jakiegokolwiek innego powodu przechowujesz dane biometryczne, możesz podlegać różnym przepisom dotyczącym prywatności i bezpieczeństwa, którym podlegają te dane. Wiele stanów uchwaliło już prawa w tym zakresie, a inne prawdopodobnie to zrobią.

Obsługa dostępu do Internetu

Małe firmy stoją przed poważnymi wyzwaniami związanymi z dostępem do Internetu i systemami informatycznymi, o których ludzie rzadko muszą myśleć i muszą podejmować różne działania, aby zapobiec powstawaniu różnych zagrożeń. Poniższe sekcje zawierają kilka przykładów.

Oddziel dostęp do Internetu dla urządzeń osobistych

Jeśli zapewniasz dostęp do Internetu osobom odwiedzającym miejsce Twojej firmy i / lub pracownikom do korzystania z ich osobistych smartfonów i tabletów w pracy, zaimplementuj ten dostęp do Internetu w innej sieci niż sieci używane do prowadzenia firmy . Większość nowoczesnych routerów oferuje taką możliwość, która zwykle występuje gdzieś w konfiguracji o nazwie takiej jak Sieć gościa.

Przynieś własne urządzenie (BYOD)

Jeśli pozwalasz pracownikom na wykonywanie czynności biznesowych na własnych laptopach lub urządzeniach mobilnych, musisz stworzyć polityki dotyczące takiej działalności i wdrożyć technologię, która ochroni Twoje dane w takim środowisku. Nie polegaj na zasadach. Jeśli nie egzekwujesz zasad za pomocą technologii, możesz doznać katastrofalnej kradzieży danych, jeśli pracownik zbankrutuje lub popełni błąd. Ogólnie rzecz biorąc, małe firmy nie powinny pozwalać na przyniesienie własnego urządzenia (BYOD) - nawet jeśli jest to kuszące. W zdecydowanej większości przypadków, gdy małe firmy pozwalają pracownikom na korzystanie z własnych urządzeń do czynności związanych z pracą, dane pozostają niewłaściwie chronione, a problemy pojawiają się, gdy pracownik odchodzi z organizacji (zwłaszcza jeśli opuszcza w mniej niż optymalnych warunkach). Wiele klawiatur Androida „uczy się” o czynnościach użytkownika podczas pisania. Chociaż takie uczenie się pomaga poprawić poprawianie pisowni i przewidywanie słów, oznacza to również, że w wielu przypadkach poufne informacje firmowe mogą zostać odczytane na urządzeniu osobistym i pozostać jako sugerowana treść,

gdy użytkownik wpisze na nim nawet po opuszczeniu pracodawcy. Jeśli zezwalasz na BYOD, pamiętaj o ustaleniu odpowiednich zasad i procedur - zarówno dotyczących użytkowania, jak i wycofywania dowolnej technologii firmowej na takich urządzeniach, a także usuwania wszelkich danych firmowych, gdy pracownik odchodzi. Opracuj pełny plan bezpieczeństwa urządzenia mobilnego, który obejmuje funkcje zdalnego czyszczenia, wymusza ochronę haseł i innych poufnych danych, przetwarza dane związane z pracą w odizolowanym obszarze urządzenia, do którego inne aplikacje nie mają dostępu (proces znany jako piaskownica), instaluje , uruchamia i aktualizuje oprogramowanie zabezpieczające zoptymalizowane pod kątem urządzeń mobilnych, zabrania pracownikom korzystania z publicznych sieci Wi-Fi w celu wykonywania wrażliwych zadań związanych z pracą, blokuje pewne działania z urządzeń, gdy są na nich dane firmowe, i tak dalej.

Obsługa dostępu przychodzącego

Jedną z największych różnic między osobami fizycznymi a firmami korzystającymi z Internetu jest często potrzeba zapewnienia przez firmę dostępu przychodzącego osobom niezaufanym. Nieznane strony muszą mieć możliwość inicjowania komunikacji, która skutkuje komunikacją z wewnętrznymi serwerami w firmie. Na przykład, jeśli firma oferuje produkty do sprzedaży online, musi umożliwić niezaufanym stronom dostęp do swojej witryny internetowej w celu dokonywania zakupów. Strony te łączą się ze stroną internetową, która musi łączyć się z systemami płatności i wewnętrznymi systemami śledzenia zamówień, nawet jeśli nie są zaufane. (Osoby fizyczne zazwyczaj nie muszą zezwalać na taki przychodzący dostęp do swoich komputerów).

Chociaż małe firmy mogą teoretycznie odpowiednio zabezpieczyć serwery internetowe, serwery poczty e-mail i tak dalej, w rzeczywistości niewiele małych firm, jeśli w ogóle, ma wystarczające zasoby, aby to zrobić, chyba że na początku zajmują się cyberbezpieczeństwem. W związku z tym rozsądne jest, aby małe firmy rozważyły użycie oprogramowania i infrastruktury innych firm, skonfigurowanych przez eksperta i zarządzanych przez ekspertów, aby hostować dowolne systemy używane do dostępu przychodzącego. Aby to zrobić, firma może przyjąć jedno lub więcej z kilku podejść:

* Wykorzystaj witrynę dużego sprzedawcy. Jeśli sprzedajesz przedmioty online i sprzedajesz tylko za pośrednictwem witryn internetowych głównych sprzedawców, takich jak Amazon, Rakuten i / lub eBay, witryny te służą jako główny bufor między systemami Twojej firmy a światem zewnętrznym. Armie bezpieczeństwa tych firm chronią przed atakami systemy skierowane do klientów. W wielu przypadkach takie systemy nie wymagają od małych firm otrzymywania komunikatów przychodzących, a kiedy to robią, komunikaty pochodzą z systemów tych sprzedawców detalicznych, a nie od opinii publicznej. Oczywiście wiele czynników wpływa na decyzję, czy sprzedawać za pośrednictwem dużego sprzedawcy - na przykład rynki internetowe pobierają wysokie prowizje. Kiedy rozważasz czynniki przy podejmowaniu takiej decyzji, pamiętaj o zaletach bezpieczeństwa.

* Skorzystaj z platformy sprzedaży detalicznej hostowanej przez inną firmę. W takim przypadku to strona trzecia zarządza większością infrastruktury i zabezpieczeń za Ciebie, ale Ty dostosowywujesz i zarządzasz rzeczywistym sklepem internetowym. Taki model nie zapewnia takiego samego poziomu izolacji od użytkowników zewnętrznych, jak poprzedni, ale oferuje znacznie większe buforowanie przed atakami, niż gdybyś sam obsługiwał własną platformę. Shopify to przykład popularnej platformy innej firmy.

* Obsługuj własną platformę obsługiwaną przez firmę zewnętrzną, która jest również odpowiedzialna za bezpieczeństwo. Takie podejście zapewnia lepszą ochronę niż samodzielne zarządzanie zabezpieczeniami, ale nie izoluje kodu od osób z zewnątrz próbujących znaleźć luki i atak. To także nakłada na Ciebie odpowiedzialność za utrzymanie i bezpieczeństwo platformy.

* Zarządzaj własnym systemem hostowanym wewnętrznie lub zewnętrznie i korzystaj z usług dostawcy usług zarządzanych, aby zarządzać bezpieczeństwem. W takim przypadku ponosisz pełną odpowiedzialność za bezpieczeństwo platformy i infrastruktury, ale większość rzeczywistej pracy wymaganej do wypełnienia tej odpowiedzialności zlecasz osobie trzeciej.

Istnieją również inne modele i wiele wariantów modeli, które wymieniam. Chociaż modele mogą być łatwiejsze do zabezpieczenia na trudniejsze do zabezpieczenia, przechodzą one również od mniej konfigurowalnych do bardziej dostosowywalnych. Ponadto, podczas gdy wcześniejsze modele mogą kosztować mniej dla mniejszych firm, koszt wcześniejszych modeli zwykle rośnie znacznie szybciej niż późniejszych w miarę rozwoju firmy. Korzystanie z dostawców zewnętrznych wiąże się z pewnym ryzykiem; Ryzyko, że mała firma nie będzie w stanie prawidłowo wdrażać zabezpieczeń i stale nimi zarządzać, jest prawdopodobnie znacznie większe niż jakiekolwiek ryzyko związane z korzystaniem z niezawodnej strony trzeciej. Oczywiście outsourcing czegokolwiek nieznanej stronie trzeciej, wobec której nie wykonałeś należytej staranności, jest niezwykle ryzykowny i nie jest zalecany.

Ochrona przed atakami typu „odmowa usługi”

Jeśli prowadzisz jakiekolwiek witryny internetowe w ramach swojej działalności, upewnij się, że masz zaimplementowaną technologię zabezpieczeń w celu ochrony przed atakami typu „odmowa usługi”. Jeśli sprzedajesz za pośrednictwem sprzedawców detalicznych, prawdopodobnie już to mają. Jeśli korzystasz z platformy chmurowej innej firmy, dostawca może ją również dostarczyć. Jeśli prowadzisz witrynę samodzielnie, powinieneś uzyskać ochronę, aby mieć pewność, że ktoś nie będzie mógł łatwo przejąć Twojej witryny - i Twojej firmy - w trybie offline.

Użyj protokołu https w swojej witrynie internetowej . Jeśli Twoja firma prowadzi witrynę internetową, pamiętaj o zainstalowaniu ważnego certyfikatu TLS / SSL, aby użytkownicy mogli komunikować się z nią za pośrednictwem bezpiecznego połączenia i wiedzieli, że witryna faktycznie należy do Twojej firmy. Niektóre systemy zabezpieczeń, które chronią przed atakami typu „odmowa usługi”, zawierają certyfikat jako część pakietu.

Zapewnienie zdalnego dostępu do systemów

Jeśli zamierzasz zapewnić pracownikom zdalny dostęp do systemów firmowych, rozważ użycie wirtualnej sieci prywatnej (VPN) i uwierzytelniania wieloskładnikowego. W przypadku dostępu zdalnego sieć VPN powinna utworzyć zaszyfrowany tunel między zdalnymi użytkownikami a firmą, a nie między użytkownikami a dostawcą VPN. Tunel chroni zarówno przed szpiegowaniem komunikacji między zdalnymi użytkownikami a firmą, a także pozwala zdalnym użytkownikom funkcjonować tak, jakby byli w biurach firmy, i korzystać z różnych zasobów biznesowych dostępnych tylko dla osób z zewnątrz. Oczywiście, jeśli korzystasz z systemów chmurowych innych firm, odpowiedni dostawcy powinni już mieć wdrożone funkcje bezpieczeństwa, które możesz wykorzystać.

Przeprowadzanie testów penetracyjnych

Pojedyncze osoby rzadko przeprowadzają testy, aby sprawdzić, czy hakerzy mogą przeniknąć do ich systemów, podobnie jak większość małych firm. Takie postępowanie może być jednak cenne - zwłaszcza w przypadku wdrażania nowego systemu lub modernizacji infrastruktury sieciowej.

Uważaj na urządzenia IoT

Wiele firm korzysta obecnie z podłączonych kamer, alarmów i tak dalej. Upewnij się, że ktoś jest odpowiedzialny za nadzorowanie bezpieczeństwa tych urządzeń, które powinny działać w oddzielnych sieciach (lub segmentach wirtualnych) niż jakiekolwiek komputery używane do prowadzenia

działalności. Kontroluj dostęp do tych urządzeń i nie zezwalaj pracownikom na podłączanie nieautoryzowanych urządzeń IoT do sieci firmowych.

Korzystanie z wielu segmentów sieci

W zależności od wielkości i charakteru Twojej firmy izolowanie różnych komputerów w różnych segmentach sieci może być rozsądne. Na przykład firma programistyczna nie powinna mieć programistów kodujących w tej samej sieci, której ludzie używają do zarządzania listą płac i rozliczeniami.

Uważaj na karty płatnicze

Jeśli akceptujesz karty kredytowe i / lub debetowe - i nie sprzedajesz za pośrednictwem strony internetowej dużego sprzedawcy - koniecznie porozmawiaj ze swoim podmiotem przetwarzającym o różnych dostępnych technologiach zapobiegających oszustwom.

Zarządzanie problemami z zasilaniem Korzystaj z zasilacza awaryjnego we wszystkich systemach, na które nie możesz sobie pozwolić nawet na chwilę. Upewnij się również, że zasilacze mogą utrzymywać systemy w stanie sprawności dłużej niż oczekiwana awaria. Jeśli na przykład sprzedajesz różne towary i usługi w handlu detalicznym online, możesz stracić bieżącą i przyszłą sprzedaż, a także ponieść uszczerbek na reputacji, jeśli Twoja zdolność do sprzedaży przestanie działać nawet na krótki czas. Nigdy nie pozwól personelowi sprzątającemu wejść do szafy serwera bez opieki - nawet na chwilę. Autor osobiście był świadkiem przypadku awarii serwera używanego przez dziesiątki osób, ponieważ administrator pozwolił personelowi sprzątającemu wejść do serwerowni bez opieki tylko po to, by później odkryć, że ktoś odłączył serwer od zasilacza awaryjnego (UPS) - urządzenia, które służy zarówno jako punkt wejścia zasilania do systemu, jak i jako zapasowa bateria - do podłączenia odkurzacza.